GFI MailEssentials™

Guida dell'amministratore

Le informazioni e il contenuto del presente documento vengono forniti esclusivamente a scopi informativi e “come sono”, senza garanzia di alcun tipo, sia espressa che implicita, ivi incluse, in via esemplificativa, tutte le garanzie implicite di commerciabilità, idoneità a soddisfare uno scopo particolare e non violazione dei diritti altrui. GFI Software non sarà ritenuta responsabile di nessun danno, inclusi danni consequenziali, che possano derivare dall’uso del presente documento. Le informazioni sono state ottenute da fonti pubblicamente disponibili. Nonostante siano stati compiuti sforzi ragionevoli al fine di garantire la precisione dei dati forniti, GFI non garantisce, promette né tantomeno assicura la completezza, la precisione, l’aggiornamento o l’adeguatezza di tali dati e non sarà ritenuta responsabile di errori di stampa. GFI non fornisce garanzie, né espresse né implicite e non si assume la responsabilità legale della precisione o della completezza delle informazioni contenute nel presente documento.

Se si ritiene che vi siano errori effettivi nel presente documento, contattarci. Provvederemo a risolvere la cosa quanto prima.

Windows, Exchange, IIS, .NET, Internet Explorer, Outlook, SQL Server e Microsoft sono marchi registrati o marchi commerciali di Microsoft Corporation negli Stati Uniti e/o in altri paesi.

Tutti i nomi di prodotti e società riportati possono essere marchi registrati dei rispettivi proprietari.

GFI MailEssentials è un copyright di GFI SOFTWARE Ltd. - 1999-2014 GFI Software Ltd. Tutti i diritti riservati.

Versione documento: 2.1.1

Ultimo aggiornamento (mese/giorno/anno): 6/25/2014

Sommario

1 Introduzione **11**

1.1 Informazioni sul presente manuale 11
1.2 Termini e convenzioni utilizzati nel presente manuale 12

2 Informazioni su GFI MailEssentials **13**

2.1 Componenti di GFI MailEssentials 13
2.2 Filtro messaggi in entrata 15
2.3 Filtro messaggi in uscita 15
2.4 Motori di scansione e filtro della posta elettronica 16
2.5 Scenari di distribuzione tipici 18
2.6 Azioni utente finale 21

3 Installazione **22**

3.1 Requisiti di sistema 22
3.2 Azioni pre-installazione 25
3.3 Procedura di installazione 40
3.4 Aggiornamento da una versione precedente 48
3.5 Azioni post-installazione 50

4 Stato di monitoraggio **54**

4.1 Dashboard 54
4.2 Rapporti 62

5 Sicurezza e-mail **74**

5.1 Motori di scansione antivirus 74
5.2 Protezione archivio informazioni 94
5.3 Scanner trojan ed eseguibili 97
5.4 Motore exploit posta 101
5.5 Strumento di disinfezione HTML 105

6 Antispam **109**

6.1 Filtri antispam 109
6.2 Operazioni antispam - cosa fare con lo spam. 148
6.3 Ordinamento filtri antispam in base alla priorità. 151
6.4 Filtraggio trasmissione SMTP 152
6.5 Spam Digest 154
6.6 Impostazioni antispam 156
6.7 SpamTag per Microsoft Outlook 162
6.8 Scansione cartella pubblica 170

7 Filtro contenuti **176**

7.1 Filtro parola chiave 176
7.2 Filtro allegati 183
7.3 Filtro avanzato contenuto 190

7.4 Motore di decompressione 196

8 Quarantena 203

8.1 Note importanti 203
8.2 Ricerca nella quarantena 203
8.3 Cartelle ricerche 209
8.4 Operazioni con i messaggi messi in quarantena 213
8.5 Feed RSS quarantena 216
8.6 Opzioni quarantena 218
8.7 Percorso e URL pubblico di Quarantine Store 225

9 Gestione posta elettronica 227

9.1 Liberatorie 227
9.2 Risposte automatiche 231
9.3 Server elenco 233
9.4 Monitoraggio posta elettronica 237

10 Impostazioni generali 239

10.1 Indirizzo e-mail amministratore 241
10.2 Abilitazione/disabilitazione dei moduli di scansione 241
10.3 Impostazioni proxy 242
10.4 Domini locali 244
10.5 Gestione utenti locali 245
10.6 Gestione licenze 246
10.7 Binding server virtuale SMTP 246
10.8 Controllo patch 247
10.9 Controllo di accesso 248

11 Argomenti vari 250

11.1 Informazioni di installazione 250
11.2 Nomi directory virtuale 251
11.3 Modalità interfaccia utente 251
11.4 Messaggi di posta elettronica non riusciti 256
11.5 Analisi 258
11.6 POP2Exchange - Download messaggi dal server POP3 259
11.7 Spostamento messaggi spam nelle cartelle della cassetta postale degli utenti 263
11.8 Spostamento spam nella cartella di Exchange 2010 266
11.9 Sincronizzazione dati di configurazione 266
11.10 Disabilitazione elaborazione messaggi di posta elettronica 278
11.11 Backup posta elettronica prima e dopo l'elaborazione 279
11.12 Porte remote 280
11.13 Monitoraggio API di scansione antivirus 281

12 Risoluzione dei problemi e supporto 286

12.1 Introduzione 286
12.2 Problemi comuni 286
12.3 Motori e filtri di scansione 288

12.4 Gestione posta elettronica 289
12.5 GFI SkyNet 290
12.6 Forum Web 290
12.7 Richiesta di supporto tecnico 290
12.8 Documentazione 291

13 Appendice - Filtro bayesiano **292**

14 Glossario **296**

15 Indice **303**

Elenco figure

Schermata 1: verifica del record MX del DNS 34
Schermata 2: Lotus Domino Administrator - fare clic sull'opzione Configurations (Configurazioni). 34
Schermata 3: Fare clic su Edit Configuration (Modifica configurazione). 35
Schermata 4: impostazioni LDAP di Lotus Domino 35
Schermata 5: abilitazione autenticazione proxy anonima 36
Schermata 6: Creazione di un nuovo database 37
Schermata 7: Caricamento risultati conversione 37
Schermata 8: Copia negli appunti di un collegamento all'applicazione corrente 38
Schermata 9: Includere tutte le cartelle pubbliche e degli altri utenti, quando viene richiesto l'elenco cartelle 38
Schermata 10: Nuovo mail-in database 39
Schermata 11: Abilitazione scansione cartella pubblica 40
Schermata 12: Inserimento dell'indirizzo di posta elettronica dell'amministratore e del codice di licenza 42
Schermata 13: Dati server SMTP e directory virtuale 43
Schermata 14: impostazioni server DNS 44
Schermata 15: impostazioni proxy 45
Schermata 16: Domini di posta elettronica in arrivo 45
Schermata 17: impostazioni server SMTP 46
Schermata 18: scelta dell'operazione antispam predefinita da effettuare 47
Schermata 19: creazione di una regola di prova per il filtro parole chiave 52
Schermata 20: messaggio di prova bloccato da Regola di prova 53
Schermata 21: Dashboard GFI MailEssentials 55
Schermata 22: I servizi di GFI MailEssentials 56
Schermata 23: Statistiche quarantena 56
Schermata 24: Grafici del dashboard 57
Schermata 25: Registri di elaborazione messaggi di posta elettronica 58
Schermata 26: filtro di elaborazione messaggi di posta elettronica 59
Schermata 27: aggiornamenti motori di scansione antivirus 60
Schermata 28: Registro eventi 61
Schermata 29: registro POP2Exchange 62
Schermata 30: creazione di un rapporto 63
Schermata 31: rapporto grafico messaggi di posta elettronica bloccati 65
Schermata 32: Ricerca nel database di creazione rapporti 68
Schermata 33: risultati di ricerca database Rapporti 69
Schermata 34: Configurazione di un database back-end Firebird 70
Schermata 35: Configurazione back-end del database SQL Server 71

Schermata 36: Rapporto flusso di comunicazione di MailInsights® 73
Schermata 37: configurazione Vipre 74
Schermata 38: azioni motore di scansione antivirus 75
Schermata 39: Schede Aggiornamenti motore 77
Schermata 40: configurazione BitDefender 78
Schermata 41: azioni motore di scansione antivirus 80
Schermata 42: Schede Aggiornamenti motore 81
Schermata 43: configurazione Kaspersky 82
Schermata 44: azioni motore di scansione antivirus 84
Schermata 45: Schede Aggiornamenti motore 85
Schermata 46: Configurazione di Avira 86
Schermata 47: azioni motore di scansione antivirus 88
Schermata 48: Schede Aggiornamenti motore 89
Schermata 49: configurazione McAfee 90
Schermata 50: azioni motore di scansione antivirus 92
Schermata 51: Schede Aggiornamenti motore 93
Schermata 52: nodo Protezione archivio informazioni 95
Schermata 53: Impostazioni VSAPI 96
Schermata 54: scanner trojan ed eseguibili: scheda Generale 98
Schermata 55: Schede Aggiornamenti motore 100
Schermata 56: configurazione exploit posta 101
Schermata 57: Azioni exploit posta 102
Schermata 58: Schede Aggiornamenti motore 103
Schermata 59: Elenco exploit posta 104
Schermata 60: pagina di configurazione strumento di disinfezione HTML 105
Schermata 61: pagina Whitelist strumento di disinfezione HTML 106
Schermata 62: esclusioni domini/IP 107
Schermata 63: proprietà SpamRazer 111
Schermata 64: scheda aggiornamenti SpamRazer 112
Schermata 65: opzioni antiphishing 114
Schermata 66: pagina Raccolta di directory 116
Schermata 67: Block list e-mail 119
Schermata 68: blocklist personale 121
Schermata 69: Block list IP 122
Schermata 70: Block list DNS IP 124
Schermata 71: Block list DNS URI 125
Schermata 72: abilitazione e configurazione delle proprietà Sender Policy Framework (SPF) 127
Schermata 73: filtro anti-spoofing GFI MailEssentials 129

Schermata 74: Esclusioni e-mail 131
Schermata 75: Opzioni di Rilevamento lingua 133
Schermata 76: opzioni di Controllo intestazione 134
Schermata 77: Rilevamento lingua 136
Schermata 78: proprietà di Controllo parole chiave spam 137
Schermata 79: proprietà analisi bayesiana 140
Schermata 80: scheda Whitelist 142
Schermata 81: whitelist personale 145
Schermata 82: scheda Generale di Nuovi mittenti 146
Schermata 83: eccezioni Nuovi mittenti 147
Schermata 84: operazioni antispam 149
Schermata 85: assegnazione priorità filtro 152
Schermata 86: proprietà di Filtraggio trasmissione SMTP 153
Schermata 87: proprietà spam digest/spam digest amministratore 154
Schermata 88: spam digest destinatario 155
Schermata 89: elenco destinatari spam digest 156
Schermata 90: Rotazione file di registro 157
Schermata 91: azioni predefinite 158
Schermata 92: impostazioni server DNS 159
Schermata 93: lingua di installazione di SpamTag e termini della licenza 166
Schermata 94: SpamTag in Microsoft Outlook 2010 169
Schermata 95: SpamTag in Microsoft Outlook 2003 169
Schermata 96: filtro contenuti: scheda Corpo - configurazione condizioni 178
Schermata 97: filtro contenuti: scheda Corpo - configurazione altre opzioni 179
Schermata 98: Filtro contenuti: scheda Utenti/cartelle 181
Schermata 99: Aggiunta di utenti a una regola di filtro dei contenuti 182
Schermata 100: filtro allegati: scheda Generale 184
Schermata 101: filtro allegati: scheda Azioni 186
Schermata 102: Filtro contenuti: scheda Utenti/cartelle 188
Schermata 103: Aggiunta di utenti a una regola di filtro dei contenuti 189
Schermata 104: aggiunta di una nuova regola di filtro avanzato contenuto 191
Schermata 105: scheda Azioni 192
Schermata 106: Filtro contenuti: scheda Utenti/cartelle 194
Schermata 107: Aggiunta di utenti a una regola di filtro dei contenuti 195
Schermata 108: controlli motore di decompressione 197
Schermata 109: area di ricerca di malware e spam 204
Schermata 110: area di ricerca di malware e spam 206
Schermata 111: area di ricerca Solo spam 208

Schermata 112: cartelle di ricerca personalizzate e predefinite 209
Schermata 113: cartelle ricerche predefinite 211
Schermata 114: Cerca risultati 213
Schermata 115: dettagli elementi messi in quarantena 214
Schermata 116: feed RSS quarantena 217
Schermata 117: opzioni spam - scheda Opzioni generali 218
Schermata 118: opzioni spam - scheda Impostazioni utente 219
Schermata 119: Modalità quarantena 221
Schermata 120: Destinatari inesistenti 223
Schermata 121: Percorso e URL pubblico di Quarantine Store 225
Schermata 122: aggiunta di una nuova liberatoria 228
Schermata 123: Liberatoria in formato HTML 229
Schermata 124: impostazioni risposta automatica 231
Schermata 125: finestra di dialogo Variabili 232
Schermata 126: creazione di un nuovo elenco 233
Schermata 127: impostazioni server SMTP perimetrali 240
Schermata 128: indicazione indirizzo e-mail amministratore 241
Schermata 129: Gestore scansione 242
Schermata 130: aggiorna le impostazioni del server proxy 243
Schermata 131: elenco domini locali 244
Schermata 132: controllo patch del prodotto 247
Schermata 133: Impostazioni Controllo di accesso 248
Schermata 134: pagina di informazioni sulla versione 250
Schermata 135: GFI MailEssentials switchboard - Modalità IU 252
Schermata 136: protezione IIS - Scheda ACL 254
Schermata 137: protezione IIS - scheda Autenticazione 255
Schermata 138: abilitazione notifica messaggi di posta elettronica non riusciti 257
Schermata 139: configura opzioni di traccia 258
Schermata 140: downloader POP3 di GFI MailEssentials 260
Schermata 141: Opzioni di connessione remota 262
Schermata 142: configurazione di un server master 270
Schermata 143: configurazione server slave 271
Schermata 144: strumento di esportazione/importazione di configurazione 273
Schermata 145: esportazione impostazioni dalla riga di comando 276
Schermata 146: Importazione impostazioni dalla riga di comando 277
Schermata 147: GFI MailEssentials Switchboard: Risoluzione dei problemi 278
Schermata 148: GFI MailEssentials Switchboard: Risoluzione dei problemi 279
Schermata 149: modifica delle porte remote 281

Schermata 150: aggiunta di contatori di performance monitor VSAPI a Windows 2008 Server 283
Schermata 151: monitoraggio file di scansione antivirus scansionati nel performance monitor di Windows Server 2008 284

1 Introduzione

1.1 Informazioni sul presente manuale

Lo scopo della presente Guida dell'amministratore è facilitare la procedura di installazione, esecuzione, configurazione e risoluzione problemi di GFI MailEssentials sulla rete. La sottostante tabella illustra i contenuti della presente guida.

Capitolo	Descrizione
Informazioni	» I componenti e strumenti alla base di GFI MailEssentials. » Funzionamento della scansione della posta in entrata e in uscita. » Panoramica dei motori che proteggono il sistema della posta. » Scenari di distribuzione tipici Per ulteriori informazioni, fare riferimento a Informazioni su GFI MailEssentials (pagina 13).
Installazione	» I vari ambienti e infrastrutture di posta supportati da GFI MailEssentials. » Prerequisiti del prodotto applicabili alla rete. » Preparazione dell'ambiente all'installazione del prodotto. » Guida attraverso le procedure di installazione e aggiornamento. » Guida dettagliata dei passaggi essenziali necessari a rendere operativo il prodotto in base alle impostazioni predefinite. » Verifica installazione e avvio del prodotto. Per ulteriori informazioni, fare riferimento a Installazione (pagina 22).
Stato di monitoraggio	» Per imparare a utilizzare il Dashboard per il monitoraggio dello stato di GFI MailEssentials in tempo reale. » Come generare rapporti grafici e statistici sull'utilizzo della posta. Per ulteriori informazioni, fare riferimento a Stato di monitoraggio (pagina 54).
Azioni utente	Vengono illustrate le azioni disponibili inGFI MailEssentials per gli utenti del dominio (non per gli amministratori del dominio) » Configurazione di whitelist e blocklist personali » Gestione dei messaggi in quarantena Per ulteriori informazioni, fare riferimento a Azioni utente finale (pagina 21).
Sicurezza e-mail	Illustra come configurare i motori di scansione antimalware. Per ulteriori informazioni, fare riferimento a Sicurezza e-mail (pagina 74).
Antispam	» Come configurare i filtri antispam. » Operazioni con i messaggi identificati come spam. » Ordinamento delle scansioni in base alla priorità di filtro. » Impostazioni generali antispam » Come gli utenti classificano i messaggi direttamente dalla loro cassetta postale (scansione cartella pubblica). Per ulteriori informazioni, fare riferimento a Antispam (pagina 109).
Filtro contenuti	Illustra la modalità di configurazione dei motori che scansionano il contenuto della posta. Per ulteriori informazioni, fare riferimento a Filtro contenuti (pagina 176).
Quarantena	Illustra la modalità di amministrazione e utilizzo della quarantena di GFI MailEssentials. Per ulteriori informazioni, fare riferimento a Quarantena (pagina 203).

Capitolo	Descrizione
Gestione posta elettronica	Per imparare a utilizzare gli strumenti nella console di Strumenti di gestione posta elettronica. » Liberatorie » risposte automatiche » server di elenco » monitoraggio posta elettronica Per ulteriori informazioni, fare riferimento a Gestione posta elettronica (pagina 227). **NOTA:** Dalla console di Gestione posta elettronica è anche possibile accedere alla funzionalità Pop2Exchange. Per ulteriori informazioni, fare riferimento a POP2Exchange - Download messaggi dal server POP3 (pagina 259).
Impostazioni generali	Illustra come personalizzare le impostazioni generali per l'ambiente in uso. Per ulteriori informazioni, fare riferimento a Impostazioni generali (pagina 239)..
Varie	Illustra varie funzioni e strumenti che è possibile utilizzare per gestire GFI MailEssentials. Per ulteriori informazioni, fare riferimento a Argomenti vari (pagina 250).
Risoluzione dei problemi	In questo capitolo viene spiegato come risolvere i problemi comuni che si possono verificare durante l'utilizzo di GFI MailEssentials. Per ulteriori informazioni, fare riferimento a Risoluzione dei problemi e supporto (pagina 286).

1.2 Termini e convenzioni utilizzati nel presente manuale

Termine	Descrizione
	Ulteriori informazioni e i riferimenti essenziali per il funzionamento di GFI MailEssentials.
	Notifiche e avvertenze importanti riguardo i potenziali problemi rilevati di frequente.
>	Istruzioni di navigazione dettagliate per accedere a una funzione specifica.
Testo in grassetto	Elementi da selezionare quali nodi, opzioni di menu o pulsanti dei comandi.
Testo in corsivo	Parametri e valori da sostituire con valori applicabili, quali percorsi personalizzati e nomi file.
`Codice`	Indica i valori di testo da immettere, come comandi e indirizzi.

Per termini tecnici e relative definizioni utilizzati nel presente manuale, consultare il Glossario.

2 Informazioni su GFI MailEssentials

Argomenti del presente capitolo:

2.1 Componenti di GFI MailEssentials 13
2.2 Filtro messaggi in entrata 15
2.3 Filtro messaggi in uscita 15
2.4 Motori di scansione e filtro della posta elettronica 16
2.5 Scenari di distribuzione tipici 18
2.6 Azioni utente finale 21

2.1 Componenti di GFI MailEssentials

2.1.1 Motore di scansione di GFI MailEssentials

Il motore di scansione di GFI MailEssentials analizza il contenuto dei messaggi di posta in entrata, in uscita e interni, utilizzando una serie di motori e filtri. Il risultato di tale analisi identifica se un messaggio deve essere bloccato o consentito.

NOTA
Durante l'installazione di GFI MailEssentials su Microsoft® Exchange server 2003, il programma effettuerà la scansione dell'archivio informazioni di Microsoft® Exchange. Se il programma viene installato su un computer Microsoft® Exchange Server 2007/2010 con i ruoli server Trasporto hub e Cassetta postale, eseguirà anche l'analisi dei messaggi di posta interni.

2.1.2 Interfaccia web di GFI MailEssentials

L'interfaccia web di GFI MailEssentials consente le seguenti operazioni:

- Monitoraggio dell'attività di scansione della posta elettronica
- Gestione dei motori di scansione e filtro
- Revisione ed elaborazione dei messaggi inseriti in quarantena
- Configurazione caratteristiche di gestione della posta elettronica
- Generazione di rapporti

2.1.3 GFI MailEssentialsSwitchboard

Utilizzare GFI MailEssentials Switchboard per:

- Configurazione avvio interfaccia utente di GFI MailEssentials
- Impostare i nomi della directory virtuale per l'interfaccia web e RSS
- Abilitare/disabilitare l'elaborazione dei messaggi di posta elettronica

- Abilitare/disabilitare l'analisi
- Impostare i backup della posta elettronica prima e dopo l'elaborazione
- Impostare il percorso di Quarantine Store e l'URL pubblico di quarantena
- Specificare l'account utente per le impostazioni 'Spostato nella cartella Exchange'
- Specificare le porte remote
- Abilitare/disabilitare le notifiche di posta non inviata

2.2 Filtro messaggi in entrata

Il filtro posta in entrata è la procedura di scansione e filtraggio dei messaggi in entrata prima del recapito agli utenti.

I messaggi in entrata vengono inoltrati a GFI MailEssentials ed elaborati come segue:

1. È possibile applicare i filtri livello SMTP (Raccolta di directory, Greylist, Block list IP e Block list DNS IP) prima della ricezione del corpo del messaggio.

2. Il messaggio viene scansionato dai motori malware e di filtro contenuti. Qualsiasi messaggio rilevato come contenente malware viene elaborato in base alle azioni configurate. Se un messaggio è ritenuto sicuro, passa alla fase successiva.

3. Il messaggio viene controllato per vedere se è indirizzato a un elenco nel server elenco. Se il messaggio corrisponde a un elenco, verrà elaborato dal server di elenco.

4. Il messaggio in entrata viene filtrato dai filtri antispam. Qualsiasi messaggio che non supera il controllo filtro antispam viene elaborato secondo quanto configurato nelle azioni antispam. Se un messaggio supera i filtri e non è identificato come spam, passa alla fase successiva.

5. Se configurate, vengono inviate le risposte automatiche al mittente.

6. Se configurato, viene eseguito il monitoraggio della posta elettronica e vengono attuate le azioni appropriate.

7. Quindi, la posta viene controllata dal filtro Nuovi mittenti.

8. Se un messaggio non viene bloccato da nessun motore di scansione o di filtro, viene inviato alla cassetta postale dell'utente.

2.3 Filtro messaggi in uscita

Il filtro dei messaggi in uscita è il processo di elaborazione dei messaggi spediti dagli utenti interni, prima che questi siano inviati tramite Internet.

All'invio di un messaggio in uscita, questo viene inoltrato a GFI MailEssentials ed elaborato come segue:

1. Il messaggio viene scansionato dai motori malware e di filtro contenuti. Qualsiasi messaggio rilevato come contenente malware viene elaborato in base alle azioni configurate. Se un messaggio è ritenuto sicuro, passa alla fase successiva.

2. I comandi remoti controllano ed eseguono eventuali comandi remoti nella posta, se presenti. Se non è presente nessun comando, il messaggio passa alla fase seguente.

3. La liberatoria corrispondente viene aggiunta al messaggio, se configurata.

4. Se configurato, viene eseguito il monitoraggio della posta elettronica e vengono attuate le azioni appropriate.

5. Se abilitata, la whitelist automatica aggiunge l'indirizzo e-mail del destinatario alla whitelist automatica. Ciò consente che le risposte dei destinatari siano inviate in automatico al mittente senza il controllo antispam.

6. Il messaggio viene inviato ai destinatari.

2.4 Motori di scansione e filtro della posta elettronica

GFI MailEssentials contiene una serie di motori di scansione e filtro per impedire a messaggi dannosi, spam e altra posta indesiderata di raggiungere gli utenti del dominio.

2.4.1 Scansione della posta elettronica dannosa

I seguenti motori scansionano e bloccano i messaggi contenenti contenuto dannoso.

Motore di scansione della posta elettronica	Descrizione
Motori di scansione antivirus	GFI MailEssentials utilizza motori antivirus multipli per la scansione di messaggi in entrata, in uscita e interni alla ricerca di virus. GFI MailEssentials viene fornito con i motori di scansione Vipre e BitDefender. È anche possibile acquistare una licenza per Kaspersky, Avira e McAfee.
Protezione archivio informazioni	Quando GFI MailEssentials è installato su un computer con Microsoft® Exchange server, Protezione archivio informazioni consente l'utilizzo dei motori di scansione antivirus per eseguire la scansione di Archivio informazioni di Microsoft® Exchange alla ricerca di virus.
Scanner trojan ed eseguibili	Scanner trojan ed eseguibili analizza e determina la funzione dei file eseguibili allegati ai messaggi. Questo scanner può successivamente inserire in quarantena qualsiasi eseguibile dall'attività sospetta, come i trojan.
Motore exploit posta	Motore exploit posta blocca gli exploit integrati nel messaggio che potrebbero essere eseguiti sul computer del destinatario al momento dell'apertura o ricezione del messaggio.
Strumento di disinfezione HTML	Strumento di disinfezione HTML scansiona e rimuove il codice di scripting presente nel corpo e negli allegati dei messaggi.

2.4.2 Motori di filtro contenuti

I seguenti motori scansionano il contenuto dei messaggi, controllando la presenza di parametri che corrispondono alle regole configurate.

Motore di scansione della posta elettronica	Descrizione
Filtro parola chiave	Filtro parole chiave consente di impostare regole che filtrano i messaggi contenenti parole chiave specifiche o una combinazione di parole chiave nel corpo o nell'oggetto del messaggio.
Filtro allegati	Filtro allegati consente la configurazione di regole per il filtraggio dei tipi di allegati dei messaggi da autorizzare e bloccare sul server di posta.
Motore di decompressione	Motore di decompressione estrae e analizza gli archivi (file compressi) allegati a un messaggio.
Filtro avanzato contenuto	Filtro avanzato contenuto consente la scansione dei dati e del contenuto dell'intestazione del messaggio, ricorrendo a condizioni di ricerca ed espressioni regolari configurabili (regex).

2.4.3 Motori filtro antispam

I seguenti motori scansionano e bloccano i messaggi spam.

FILTRO	DESCRIZIONE	ABILITATO PER IMPOSTAZIONE PREDEFINITA
SpamRazer	Un motore antispam che riconosce se un messaggio di posta elettronica è spam attraverso impronte digitali, reputazione e analisi del contenuto dei messaggi.	Sì
Antiphishing	Blocca i messaggi che contengono collegamenti ai corpi del messaggio che indirizzano a siti noti di phishing o che contengono parole chiave di phishing tipiche.	Sì
Raccolta di directory	Gli attacchi di Raccolta di directory si verificano quando gli spammer cercano di indovinare gli indirizzi di posta allegando i nomi utente noti al dominio della vittima. La maggioranza degli indirizzi di posta elettronica è inesistente.	Sì (solo se GFI MailEssentials è installato in un ambiente Active Directory)
Block list e-mail	La Block list e-mail è un database personalizzato di indirizzi di posta elettronica e domini da cui non si desidera ricevere alcun messaggio.	Sì
Block list IP	La Block list IP è un database personalizzato di indirizzi IP da cui non si desidera ricevere alcun messaggio.	No
Block list DNS IP	Block list DNS IP controlla l'indirizzo IP del server di invio della posta con un elenco pubblico di server di posta noti per l'invio di spam.	Sì
Block list DNS URI	Arresta i messaggi che contengono collegamenti a domini elencati nelle block list URI spam.	Sì
Sender Policy Framework	Questo filtro utilizza i record SPF per arrestare i messaggi inviati da indirizzi IP falsificati, identificando se l'indirizzo IP del mittente è autorizzato.	No
Anti-spoofing	I messaggi ricevuti con un indirizzo e-mail del mittente e che sembrano provenire dal proprio dominio vengono controllati da GFI MailEssentialssulla base di un elenco di indirizzi IP. Se l'indirizzo IP del mittente non è presente nell'elenco di indirizzi IP del server del proprio dominio, il messaggio verrà bloccato.	No
Rilevamento lingua	Determina la lingua del testo del corpo del messaggio ed è configurabile per il blocco di determinate lingue.	No
Controllo intestazione	Il filtro Controllo intestazione analizza l'intestazione e-mail per identificare i messaggi spam.	No
Controllo parole chiave spam	Questo filtro consente l'identificazione dello spam sulla base di parole chiave all'interno del messaggio ricevuto.	No
Analisi bayesiana	Un filtro antispam che può essere addestrato per determinare con precisione se un messaggio è spam in base a quanto rilevato in precedenza.	No

2.4.4 Filtri che vengono eseguiti a livello SMTP

I seguenti motori scansionano e bloccano i messaggi durante la trasmissione SMTP prima del ricevimento del messaggio. Per ulteriori informazioni, fare riferimento a Filtraggio trasmissione SMTP (pagina 152).

FILTRO	DESCRIZIONE	ABILITATO PER IMPOSTAZIONE PREDEFINITA
Block list IP	La Block list IP è un database personalizzato di indirizzi IP da cui non si desidera ricevere alcun messaggio.	No
Raccolta di directory	Gli attacchi di Raccolta di directory si verificano quando gli spammer cercano di indovinare gli indirizzi di posta allegando i nomi utente noti al dominio della vittima. La maggioranza degli indirizzi di posta elettronica è inesistente.	No
Block list DNS IP	Block list DNS IP controlla l'indirizzo IP del server di invio della posta con un elenco pubblico di server di posta noti per l'invio di spam.	Sì
Greylist	Il filtro greylist blocca temporaneamente i messaggi di posta in arrivo ricevuti da mittenti sconosciuti. Normalmente, i sistemi di posta attendibili ritentano l'invio dopo alcuni minuti, gli spammer invece ignorano tali messaggi di errore.	No

2.4.5 Altri motori

I seguenti motori aiutano a identificare i messaggi sicuri.

FILTRO	DESCRIZIONE	ABILITATO PER IMPOSTAZIONE PREDEFINITA
Whitelist	La whitelist contiene gli elenchi dei criteri che identificano la posta attendibile. Le e-mail che rispettano tali criteri non saranno scansionate dai filtri antispam e verranno sempre recapitate al destinatario.	Sì
Nuovi mittenti	Il filtro Nuovi mittenti identifica i messaggi di posta elettronica inviati da mittenti ai quali non sono mai stati inviati messaggi.	No

2.5 Scenari di distribuzione tipici

Il presente capitolo illustra i diversi scenari sulle modalità di installazione e configurazione di GFI MailEssentials.

2.5.1 Installazione diretta su Microsoft® Exchange server

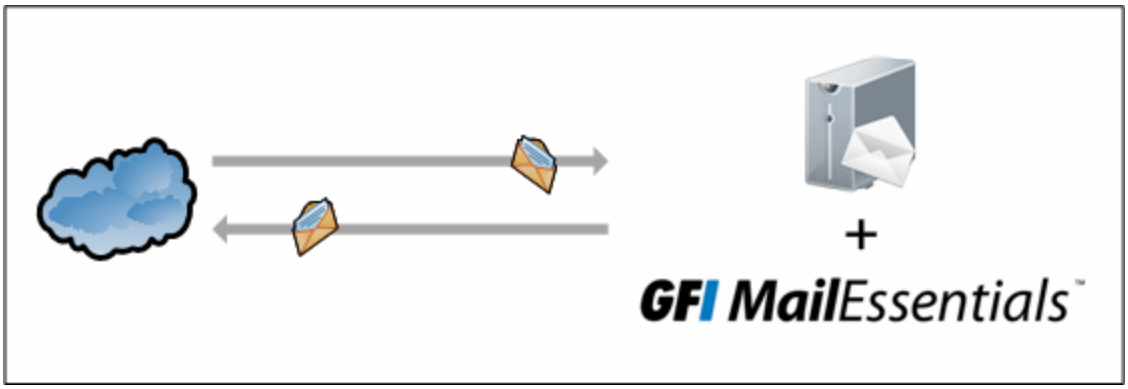


Figura 1: Installazione di GFI MailEssentials su Microsoft® Exchange server

GFI MailEssentials può essere installato direttamente su Microsoft® Exchange Server 2003 o versioni successive, senza ulteriori configurazioni aggiuntive.

Negli ambienti Microsoft® Exchange 2007/2010, GFI MailEssentials può essere installato solo sui server con i seguenti ruoli:

- Ruolo Edge Server o
- Ruolo Trasporto Hub, o
- Ruolo Trasporto Hub e Cassetta postale: con questa configurazione GFI MailEssentials può scansionare anche i messaggi interni alla ricerca di virus.

Negli ambienti Microsoft® Exchange 2013, GFI MailEssentials può essere installato solo sui server con i seguenti ruoli:

- Ruolo Trasporto Edge o
- ruolo Cassetta postale.

> **NOTA**
> GFI MailEssentials supporta una serie di server di posta ma può essere installato solo sullo stesso computer dove è presente Microsoft® Exchange. Per gli altri server di posta, ad esempio Lotus Domino, installare GFI MailEssentials su un computer separato.

2.5.2 Installazione in un gateway di posta o su un relay server/server perimetrale

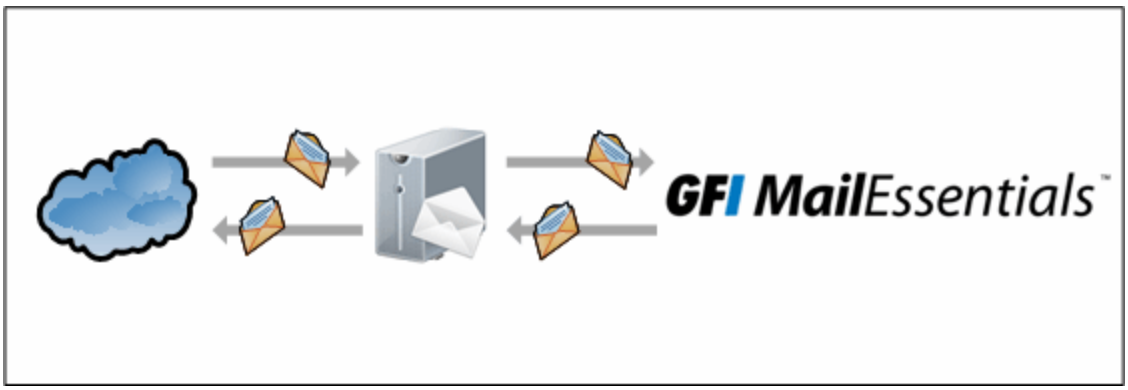


Figura 2: Installazione di GFI MailEssentials su un gateway di posta/relay server

Questa configurazione viene solitamente utilizzata per filtrare lo spam in un computer separato, solitamente installato in una DMZ. In questo ambiente viene impostato un server (noto anche come gateway/server perimetrale) per inoltrare i messaggi al server di posta. GFI MailEssentials è installato sul gateway/server perimetrale, così da filtrare lo spam e il malware della posta prima che raggiunga il server di posta.

Questo metodo consente di escludere i messaggi bloccati prima che siano ricevuti dal server di posta, riducendo in tal modo il traffico di posta non necessario. Inoltre, offre una tolleranza di errore aggiuntiva: quando il server di posta è irraggiungibile, è comunque possibile ricevere i messaggi, poiché questi vengono messi in coda sul computer dove è installato GFI MailEssentials.

Durante l'installazione in un server separato, diverso dal server di posta, è necessario prima configurare tale computer affinché agisca da gateway, (detto anche "Smart host" o server "Inoltro posta"). Ciò significa che tutti i messaggi di posta in entrata devono passare attraverso GFI MailEssentials per essere scansionati, prima del loro inoltro al server della posta per la distribuzione. Per i messaggi in uscita, il server della posta deve inoltrare tutti i messaggi in uscita al computer gateway affinché siano scansionati prima di essere inviati a destinazione.

Se si utilizza un firewall, una buona soluzione è quella di distribuire GFI MailEssentials nella DMZ. Quando GFI MailEssentials viene installato nella rete perimetrale (detta anche DMZ, zona demilitarizzata), fungerà da smart host/server di inoltro della posta.

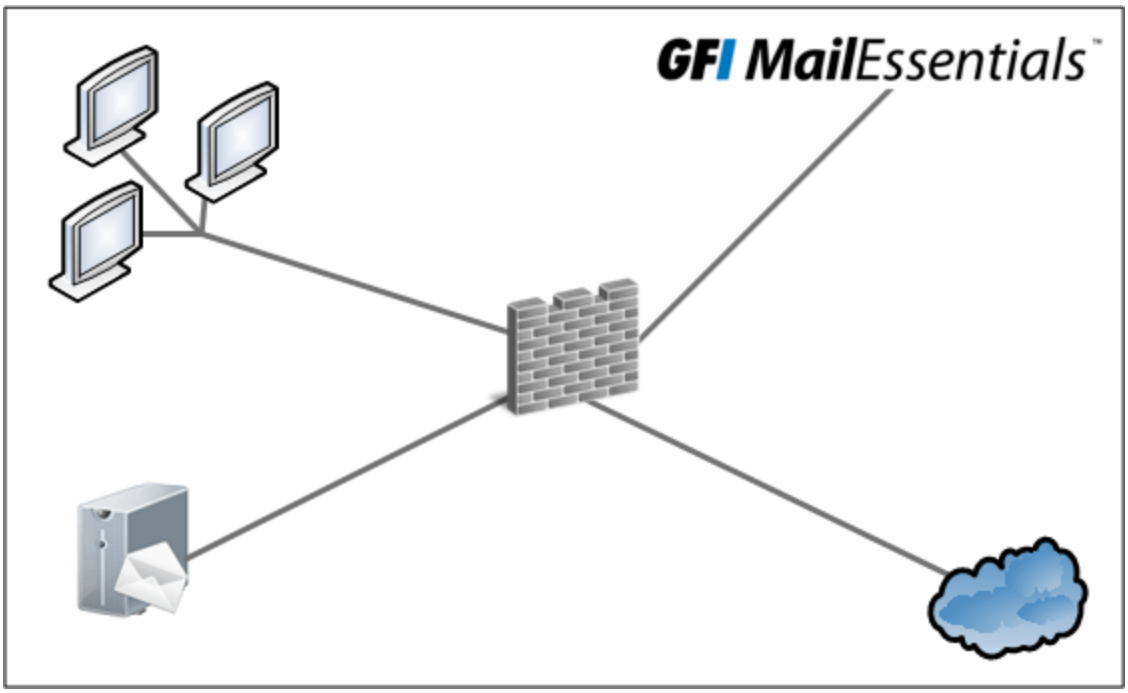


Figura 3: installazione di GFI MailEssentials su un computer separato o in una DMZ

NOTA
Se GFI MailEssentials è installato sul server perimetrale, si possono utilizzare i filtri antispam che vengono eseguiti a livello SMTP : raccolta di directory e greylist.

NOTA
Negli ambienti Microsoft® Exchange Server 2007/2010, i server di inoltro della posta di una DMZ possono eseguire Microsoft® Exchange Server 2007/2010 con il ruolo server Trasporto Edge.

NOTA

Configurare il servizio SMTP di IIS per l'inoltro dei messaggi di posta al server della posta e configurare il record MX del dominio affinché indichino il computer gateway. Per ulteriori informazioni, fare riferimento a Installazione in un gateway di posta o su un relay server/server perimetrale (pagina 26).

2.6 Azioni utente finale

GFI MailEssentials utilizza i gruppi di Active Directory per determinare ciò che viene visualizzato agli utenti connessi al momento di accedere a GFI MailEssentials. Se l'utente attualmente connesso fa parte del gruppo amministratori, allora GFI MailEssentials si carica con tutte le opzioni di configurazione che abilitano la configurazione di GFI MailEssentials. Se l'utente attualmente connesso fa parte del gruppo utenti, allora GFI MailEssentials viene caricato con solo un numero limitato di opzioni che consente all'utente attualmente connesso di amministrare la propria quarantena e le whitelist/blocklist personali. L'URL utilizzato per connettersi a GFI MailEssentials è sempre il medesimo, a prescindere dal fatto che l'utente attualmente connesso faccia parte del gruppo amministratore o del gruppo Active Directory.

NOTA

Le azioni degli utenti sono disponibili solo se GFI MailEssentials è configurato per l'utilizzo della modalità IIS. Per ulteriori informazioni, fare riferimento a Modalità interfaccia utente (pagina 251).

Elenco di funzionalità disponibili per gli account degli utenti:

Funzione	Descrizione
Whitelist e block list personale	Gli utenti possono configurare un elenco integrativo di indirizzi di posta inseriti nella whitelist e nella block list, in aggiunta all'elenco impostato dall'amministratore di sistema. Questa funzione è disponibile solo quando la Whitelist personale e/o la Block list personale sono abilitate. Per impostazione predefinita, queste opzioni non sono abilitate.
Ricerca in quarantena	Consente agli utenti di accedere e gestire i messaggi di spam che sono state inserite in quarantena. Gli utenti possono cercare, visualizzare e quindi approvare o eliminare i messaggi inseriti in quarantena. Per utilizzare questa funzione, l'azione dei filtri antispam deve essere configurata per inserire in quarantena i messaggi di spam. Gli utenti non possono gestire le e-mail di malware in quarantena per via dei rischi di sicurezza contenuti.
SpamTag	Gli utenti possono utilizzare il componente aggiuntivo SpamTag in Microsoft Outlook per gestire le loro preferenze di gestione dei messaggi di spam. SpamTag deve essere installato nel computer degli utenti per poter essere accessibile tramite Microsoft Outlook. **NOTA:** Questa caratteristica non è disponibile per gli utenti nell'interfaccia web di GFI MailEssentials. Per ulteriori informazioni, fare riferimento a SpamTag per Microsoft Outlook (pagina 162).
MailInsights®	MailInsights® è una funzionalità di creazione rapporti che offre una rappresentazione grafica dei primi 20 contatti con cui un utente ha comunicato nei 30 giorni precedenti.

Per ulteriori informazioni sulle modalità di utilizzo di GFI MailEssentials da parte degli utenti finali, fare riferimento al Manuale utente finale di GFI MailEssentials.

3 Installazione

Lo scopo del presente capitolo è facilitare l'installazione di GFI MailEssentials sulla rete con il minimo impegno nella configurazione.

Argomenti del presente capitolo:

3.1 Requisiti di sistema **22**

3.2 Azioni pre-installazione **25**

3.3 Procedura di installazione **40**

3.4 Aggiornamento da una versione precedente **48**

3.5 Azioni post-installazione **50**

3.1 Requisiti di sistema

3.1.1 Requisiti hardware

I requisiti hardware minimi per GFI MailEssentials sono:

Processore

- Minimo: 2 Ghz
- Consigliato: 2 GHz con core multipli

Memoria disponibile (RAM)

- Minimo: 1,2 GB
- Consigliato: 1,5 GB

Spazio libero su disco

- Minimo: 6 GB
- Consigliato: 10 GB

> **NOTA**
> I requisiti hardware dipendono da una varietà di fattori tra cui volume della posta e numero di motori antivirus abilitati in GFI MailEssentials. I requisiti indicati sopra sono obbligatori solo per GFI MailEssentials.

3.1.2 Requisiti software

Sistemi operativi supportati

» Windows® Server 2003 Standard o Enterprise (x86 o x64)(compreso R2) o versioni successive (comprese le edizioni Microsoft® Windows Server 2012 - Standard e DataCenter).

» Windows Small Business Server 2003/2008/2011

Server di posta elettronica supportati

GFI MailEssentials può essere installato sui seguenti server di posta senza ulteriori configurazioni.

» Microsoft® Exchange Server 2013

> **NOTA**
> Information Store Protection (VSAPI) non è supportato su Microsoft® Exchange Server 2013, in quanto VSAPI è stato rimosso da Microsoft® Exchange Server 2013.

» Microsoft® Exchange Server 2010

» Microsoft® Exchange Server 2007 SP1 o versioni successive

» Microsoft® Exchange Server 2003

Per ulteriori informazioni, fare riferimento a Installazione su Microsoft® Exchange Server (pagina 26).

GFI MailEssentials può essere installato anche in un ambiente con un server di posta conforme a SMTP. In questo caso, GFI MailEssentials deve essere installato sul gateway/server perimetrale, così da filtrare lo spam prima che raggiunga il server di posta.

Per ulteriori informazioni, fare riferimento a Installazione in un gateway di posta o su un relay server/server perimetrale (pagina 26).

Browser Internet supportati

GFI MailEssentialspuò essere utilizzato con i seguenti browser Internet:

» Microsoft Internet Explorer 8 o versioni successive

» Google Chrome versione 22.0.1229.94 (10 ottobre 2012) o successive

» Mozilla Firefox versione 16.0.2 (26 ottobre 2012) o versioni successive.

Altri componenti obbligatori

» Servizio Web Internet Information Services (IIS®)

» Servizio SMTP Internet Information Services (IIS®): eccetto quando si installa su Microsoft® Exchange 2007/2010/2013 server

» Microsoft.NET® Framework 4

» Windows Communication Foundation HTTP Activation - necessaria per l'utilizzo del plugin di SpamTag per Microsoft Outlook

» Servizi ruolo Autenticazione e Contenuto statico di Windows®: obbligatori al momento di installare su Microsoft® Windows Server 2008/2008R2

» MSMQ - Servizio Microsoft® Messaging Queuing: per ulteriori informazioni fare riferimento a:

- Installazione di MSMQ su Windows Server 2012
- Installazione di MSMQ su Windows Server 2008
- Installazione di MSMQ su Windows Server 2003

NOTA
Per ulteriori informazioni sulla modalità di installazione dei prerequisiti su Microsoft Windows® Server 2008, fare riferimento a:
http://go.gfi.com/?pageid=ME_Win2008
Per ulteriori informazioni sulla modalità di installazione dei prerequisiti su Microsoft Windows® Server 2012, fare riferimento a:
http://go.gfi.com/?pageid=ME_Win2012

NOTA
Protezione archivio informazioni di GFI MailEssentials non può essere utilizzato se sono registrati altri software per l'utilizzo di Microsoft® Exchange VSAPI.

NOTA
GFI MailEssentials può essere installato anche in ambienti virtuali come Microsoft® Hyper-V e software di virtualizzazione VMWare.

» La risorse del gruppo di cluster Microsoft Virtual Server con un cluster disco fisico. È obbligatoria SOLO per gli ambienti che eseguono i cluster Microsoft® Exchange 2003. Per ulteriori informazioni, fare riferimento a Cluster di Microsoft® Exchange 2003 (pagina 30).

NOTA
Per ulteriori informazioni su come creare un gruppo di risorse per un server virtuale di Exchange in un cluster di server di Windows, fare riferimento a: http://go.gfi.com/?pageid=ME_Clusterresourcegrouphowto

3.1.3 Software antivirus e di backup

Il software antivirus e di backup può provocare malfunzionamenti in GFI MailEssentials. Ciò accade quando tale software nega l'accesso ad alcuni file necessari a GFI MailEssentials.

Disabilitare la scansione delle seguenti cartelle da parte di software antivirus e di backup di terze parti:

Installazioni a 32 bit (x86)	Installazioni a 64 bit (x64)
<..\Programmi\File comuni\GFI>	<..\Program Files (x86)\Common Files\GFI>
<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\	
<..\Inetpub\mailroot>: se installato in un computer gateway.	
<..\Program Files\Exchsrvr\Mailroot>: se installato sul medesimo computer di Microsoft® Exchange 2003,	
<..\Program Files\Microsoft\Exchange Server\TransportRoles>: se installato sul medesimo computer di Microsoft® Exchange 2007.	

Installazioni a 32 bit (x86)	Installazioni a 64 bit (x64)
<..*Program Files\Microsoft\Exchange Server\V14\TransportRoles*>: se installato sul medesimo computer di Microsoft® Exchange 2010.	
<..*Program Files\Microsoft\Exchange Server\V15\TransportRoles*>: se installato sul medesimo computer di Microsoft® Exchange 2013.	

3.1.4 Impostazioni delle porte del firewall

Configurare il firewall in uso in modo da autorizzare le porte utilizzate da GFI MailEssentials.

Porta	Descrizione
53 - DNS	Utilizzata dai seguenti filtri antispam: » Block list DNS IP » SpamRazer » Block list DNS URI
20 e 21 - FTP	Utilizzata da GFI MailEssentials per connettersi a **ftp.gfi.com** e recuperare le informazioni più recenti di versione del prodotto.
80 - HTTP	Utilizzate da GFI MailEssentials per scaricare gli aggiornamenti e le patch prodotto di: » SpamRazer » Antiphishing » Analisi bayesiana » File definizioni antivirus » Scanner trojan ed eseguibili » Motore exploit posta GFI MailEssentials scarica dai seguenti percorsi: » http://update.gfi.com » http://update.gfisoftware.com » http://support.gfi.com » *.mailshell.com » *.spamrazer.gfi.com **NOTA:** GFI MailEssentials può anche essere configurato per scaricare gli aggiornamenti mediante un server proxy. Per ulteriori informazioni, fare riferimento a Impostazioni proxy (pagina 242).
9090, 9091 - Comunicazione remota	Queste porte vengono utilizzate per la comunicazione tra i processi. Poiché tutti i processi di GFI MailEssentials vengono eseguiti sul medesimo server, non è necessario apportare configurazioni firewall. **NOTA:** Assicurarsi che non vi siano applicazioni in ascolto su queste porte, ad eccezione di GFI MailEssentials. Se vi sono altre applicazioni che utilizzano queste porte, sarà possibile modificare le porte. Per ulteriori informazioni, fare riferimento a Porte remote (pagina 280).
389/636 - LDAP/LDAPS	Questa porta viene utilizzati nei seguenti scenari: » **Ambiente Microsoft® Exchange**: obbligatoria se il server che esegue GFI MailEssentials non ha accesso/non può ottenere l'elenco di utenti da Active Directory, ad esempio, in un ambiente DMZ o in altri ambienti che non utilizzano Active Directory. » **Ambiente server di posta Lotus Domino mail**: obbligatoria per ottenere gli indirizzi di posta dal server Lotus Domino. » **Altri ambienti server di posta SMTP**: obbligatoria per ottenere gli indirizzi di posta dal server SMTP.

3.2 Azioni pre-installazione

Prima di installare GFI MailEssentials, preparare l'ambiente alla distribuzione.

Argomenti del presente capitolo:

» Installazione su Microsoft Exchange server

» Installazione in un gateway di posta o su un relay server/server perimetrale

» Cluster di Microsoft Exchange 2003

» Lotus Domino

3.2.1 Installazione su Microsoft® Exchange Server

Quando si installa GFI MailEssentials sul medesimo server di Microsoft® Exchange 2003 o versioni successive, non sono necessarie azioni né configurazioni pre-installazione.

Negli ambienti Microsoft® Exchange 2007/2010, GFI MailEssentials può essere installato solo sui server con i seguenti ruoli:

» Ruolo Edge Server o

» Ruolo Trasporto Hub, o

» Ruolo Trasporto Hub e Cassetta postale: con questa configurazione GFI MailEssentials può scansionare anche i messaggi interni alla ricerca di virus.

Negli ambienti Microsoft® Exchange 2013, GFI MailEssentials può essere installato solo sui server con i seguenti ruoli:

» Ruolo Trasporto Edge o

» ruolo Cassetta postale.

3.2.2 Installazione in un gateway di posta o su un relay server/server perimetrale

GFI MailEssentials può essere installato:

» in un server perimetrale (ad esempio, una DMZ)

» come relay server della posta tra il server perimetrale SMTP (gateway) e il server di posta

Questa configurazione viene solitamente utilizzata per filtrare lo spam in un computer separato, solitamente installato in una DMZ. In questo ambiente viene impostato un server (noto anche come gateway/server perimetrale) per inoltrare i messaggi al server di posta. GFI MailEssentials è installato sul gateway/server perimetrale, così da filtrare lo spam e il malware della posta prima che raggiunga il server di posta.

GFI MailEssentials utilizza il servizio SMTP di IIS come server SMTP, pertanto anche il servizio SMTP di IIS deve essere configurato per essere utilizzato come relay server della posta. A tale scopo, procedere come segue:

Passaggio 1: abilitazione servizio SMTP di IIS

Passaggio 2: creazione di domini SMTP per l'inoltro della posta

Passaggio 3: abilitazione inoltro della posta su Microsoft® Exchange server

Passaggio 4: protezione del relay server della posta SMTP

Passaggio 5: abilitazione del server della posta per l'inoltro dei messaggi tramite gateway

Passaggio 6: aggiornamento del record MX del dominio affinché indirizzi al relay server della posta

Passaggio 7: verifica del nuovo relay server della posta

Passaggio 1: abilitazione servizio SMTP di IIS

Windows Server 2003

1. Fare clic su **Start > Pannello di controllo > Installazione applicazioni > Aggiungi/rimuovi componenti Windows**.
2. Selezionare **Server applicazioni** e fare clic su **Dettagli**.
3. Selezionare **Internet Information Services (IIS)** e fare clic su **Dettagli**.
4. Selezionare l'opzione **Servizio SMTP** e fare clic su **OK**.
5. Per completare la configurazione, fare clic su **Avanti**.

Windows Server 2008

1. Avviare Server Manager di Windows.
2. Navigare al nodo **Funzionalità** e selezionare **Aggiungi funzionalità**.
3. Da **Aggiunta guidata funzionalità** selezionare **Server SMTP**.

> **NOTA**
> La funzionalità server SMTP potrebbe richiedere l'installazione di servizi e funzionalità aggiuntive per il ruolo. Per procedere con l'installazione, fare clic su **Aggiungi servizi ruolo necessari**.

4. Nelle schermate successive, fare clic su **Avanti** per configurare i servizi e funzionalità ruolo necessari e selezionare **Installa** per avviare l'installazione.
5. Per finalizzare la configurazione, fare clic su **Chiudi**.

Passaggio 2: creazione di domini SMTP per l'inoltro della posta

1. Accedere a **Pannello di controllo > Strumenti di amministrazione > Gestione Internet Information Services (IIS).**

2. Nel riquadro a sinistra, espandere il nodo rispettivo del server. Fare clic con il pulsante destro su **Server virtuale SMTP predefinito**, quindi selezionare **Proprietà**.

4. Espandere il nodo **Server virtuale SMTP predefinito**.

5. Fare clic con il pulsante destro del mouse su **Domini** e selezionare **Nuovo > Dominio**.

6. Selezionare **Remoto** e fare clic su **Avanti**.

7. Indicare il nome di dominio dell'organizzazione (ad esempio, provail.miodominio.com), quindi fare clic su **Fine**.

Passaggio 3: abilitazione inoltro della posta su Microsoft® Exchange server

1. Fare clic con il pulsante destro del mouse sul nuovo dominio, quindi selezionare **Proprietà**.

2. Selezionare **Consenti l'inoltro della posta in arrivo al dominio specificato**.

3. Selezionare **Inoltra tutta la posta a SmartHost** e indicare l'indirizzo IP del server che gestisce i messaggi in questo dominio. Gli indirizzi IP devono essere racchiusi da parentesi quadre, ad esempio, `[123.123.123.123]`, così da essere esclusi da tutti i tentativi di ricerca del DNS.

4. Fare clic su **OK** per completare la configurazione.

Passaggio 4: protezione del relay server della posta SMTP

In assenza di protezione, il relay server della posta può essere sfruttato come inoltro aperto per lo spam. Per impedirlo, si consiglia di indicare i server della posta che possono inoltrare i messaggi tramite questo relay server: ad esempio, consentire solo a server specifici di utilizzare questa configurazione di inoltro della posta). A tal fine:

1. Accedere a **Pannello di controllo > Strumenti di amministrazione > Gestione Internet Information Services (IIS).**

2. Nel riquadro a sinistra, espandere il nodo rispettivo del server. Fare clic con il pulsante destro su **Server virtuale SMTP predefinito**, quindi selezionare **Proprietà**.

3. Dalla scheda **Accesso**, selezionare **Relay**.

4. Selezionare **Solo i computer indicati nell'elenco** e fare clic su **Aggiungi**.

5. Indicare gli indirizzi IP dei server di posta interni ai quali è consentito inoltrare i messaggi attraverso il relay server della posta. È possibile indicare:

» Computer singoli: autorizzare un computer specifico per l'inoltro della posta attraverso questo server. Utilizzare il pulsante Ricerca DNS per cercare un indirizzo IP di un host specifico.

» Gruppo di computer: autorizzare computer specifici per l'inoltro della posta attraverso questo server.

» Dominio: consentire ai computer del dominio indicato di inoltrare i messaggi tramite questo server.

> **NOTA**
> L'opzione **Dominio** aggiunge un overhead di elaborazione che può peggiorare le prestazioni del servizio SMTP. Ciò è dovuto alle procedure di ricerca DNS inverso attivate su tutti gli indirizzi IP (all'interno del dominio) che tentano l'inoltro di messaggi attraverso questo relay server.

Passaggio 5: abilitazione del server della posta per l'inoltro dei messaggi tramite GFI MailEssentials

Microsoft® Exchange Server 2003

Configurare i connettori SMTP che inoltrano tutti i messaggi a GFI MailEssentials.

1. Avviare **Gestore di sistema di Exchange**.

2. Fare clic con il pulsante destro del mouse su **Connettori**, selezionare **Nuovo > Connettore SMTP**, quindi indicare un nome per il connettore.

3. Selezionare l'opzione **Invia tutta la posta tramite i seguenti SmartHost** e digitare l'indirizzo IP del relay server di GFI MailEssentials racchiuso tra parentesi quadre, ad esempio `[123.123.1.123]`.

4. Fare clic su **Aggiungi** e selezionare il relay server della posta di GFI MailEssentials.

5. Fare clic su **OK**.

6. Selezionare la scheda **Spazio indirizzo**.

7. Fare clic su **Aggiungi**, selezionare **SMTP** e scegliere **OK**.

8. Immettere il nome del dominio e fare clic su **OK**.

9. Selezionare **Consenti l'inoltro dei messaggi ai domini**.

10. Fare clic su **OK**.

Lotus Notes

Per ulteriori informazioni su come configurare il routing Lotus Domino, fare riferimento alla Guida di installazione (Domino).

Server di posta SMTP/POP3

Configurare il server di posta per l'inoltro di tutta la posta in entrata e in uscita tramite GFI MailEssentials. Nel programma di configurazione del server di posta, utilizzare questa opzione per inoltrare tutta la posta in uscita tramite un altro server di posta (questa opzione viene solitamente considerata simile a **Inoltra tutti i messaggi all'host**. Inserire il nome del computer o l'indirizzo IP del computer che esegue GFI MailEssentials. Salvare le nuove impostazioni e riavviare il server di posta.

Passaggio 6: aggiornamento del record MX del dominio affinché indirizzi al relay server della posta

Aggiornare il record MX del dominio affinché indirizzi all'IP del nuovo relay server della posta. Se il server DNS è gestito dall'ISP, chiedere all'ISP di aggiornare il record MX.

> **NOTA**
> Se il record MX non è aggiornato, tutti i messaggi verranno inoltrati direttamente al server di posta, dunque ignorando GFI MailEssentials.

Verifica del corretto aggiornamento del record MX

Per verificare se è stato aggiornato il record MX:

1. Dal prompt dei comandi, digitare `nslookup` e premere **Invio**.

2. Digitare `set type=mx`, quindi premere **Invio**.

3. Indicare il nome dominio di posta, quindi premere **Invio**.

Il record MX deve restituire gli indirizzi IP dei relay server della posta.

Passaggio 7: verifica del nuovo relay server della posta

Prima di procedere con l'installazione di GFI MailEssentials, verificare che il nuovo relay server della posta funzioni correttamente.

Verifica connessione in entrata SMTP di IIS

1. Inviare un messaggio da un account 'esterno' (ad esempio da un account Gmail) a un indirizzo di posta/utente interno.

2. Assicurarsi che il destinatario previsto riceva il messaggio di prova nel rispettivo client di posta.

Verifica connessione in uscita SMTP di IIS

1. Inviare un messaggio da un account 'interno' a un account esterno (ad esempio Gmail).
2. Assicurarsi che l'utente esterno/destinatario previsto abbia ricevuto il messaggio di prova.

> **NOTA**
> È anche possibile utilizzare Telnet per inviare manualmente il messaggio di prova e ottenere maggiori informazioni per la risoluzione dei problemi. Per ulteriori informazioni, fare riferimento a:
> http://go.gfi.com/?pageid=ME_TelnetPort25

3.2.3 Cluster di Microsoft® Exchange 2003

Il presente argomento contiene le istruzioni sulla modalità di installazione e disinstallazione di GFI MailEssentials sui cluster Microsoft® Exchange 2003.

Un cluster è un gruppo di server, noti a livello tecnico come nodi, che operano in modo collettivo come un server unico. Questi ambienti offrono meccanismi di disponibilità elevata e failover per consentire la disponibilità costante delle risorse e applicazioni, incluse le infrastrutture esistenti di posta. Se uno dei nodi del cluster genera un errore o non è disponibile, le risorse e le altre applicazioni verranno passate a un altro nodo del cluster.

> **NOTA**
> GFI MailEssentials può essere installato solo in un ambiente di cluster attivo/passivo. In un cluster attivo/passivo, il meccanismo di failover assicura che in caso di errore di un cluster attivo, uno dei nodi passivi disponibili diventi attivo (assume il ruolo del nodo con errore).

Per installare GFI MailEssentials in un cluster Microsoft® Exchange Server 2000/2003, assicurarsi che:

» Tutte le applicazioni in esecuzione siano chiuse.

» Microsoft® Exchange Server 2000/2003 sia installato in modalità cluster.

» Esista una risorsa di gruppo di cluster del server virtuale di Exchange che includa, tra le altre cose, una risorsa cluster disco fisico.

» Tutti i nodi del cluster siano disattivati, ad eccezione di quello dove sarà installato per primo GFI MailEssentials.

1. Avviare la procedura di installazione e assicurarsi che:
   - Tutti i file siano installati sul disco rigido condiviso
   - Si sta eseguendo l'installazione sul sito web predefinito del computer
2. Al termine, avviare il sito web predefinito tramite Gestore di IIS.
3. Andare a **Pannello di controllo > Strumenti di amministrazione > Amministrazione cluster** e creare un nuovo gruppo di risorse (fare clic con il pulsante destro del mouse su **Gruppi > Nuovo > Gruppo**).

4. Digitare `GFI MailEssentials` come nome e `Servizi per GFI MailEssentials` come descrizione. Fare clic su **Avanti**.

5. Spostare tutti i nodi disponibili in **Proprietari preferiti** e fare clic su **Fine**.

6. Fare clic con il pulsante destro del mouse su **GFI MailEssentials > Nuovo > Risorsa**.

7. Impostare il nome come `GFI List Server`.

8. Impostare Tipo di risorsa su Servizio generico e fare clic su **Avanti**.

9. Impostare tutti i nodi disponibili sui proprietari possibili, quindi fare clic su **Avanti**.

10. Fare clic su **Avanti**.

11. Impostare il nome del servizio su `listserv` e fare clic su Avanti.

12. Fare clic su **Fine**.

13. Ripetere i passaggi da 7 a 12 con i seguenti dati:

Nome	Nome servizio
GFI MailEssentials AS Scan Engine	gfiscans
GFI MailEssentials Attendant	gfimesattendant
GFI MailEssentials Autoupdater	gfimesavupdate
GFI MailEssentials AV Scan Engine	GFIScanM
GFI MailEssentials Backend	gfimesbackend
GFI MailEssentials Enterprise Transfer	gfimetrxsvc
GFI MailEssentials Legacy Attendant	gfiasmsecatt
GFI MailEssentials Quarantine Action Services	gfimesqashost
GFI POP2Exchange	gfipop2exch

14. Al completamento, portare online il gruppo GFI MailEssentials.

15. Arrestare il nodo e attivarne uno nuovo.

16. Ripetere i passaggi 1 e 2 per tutti i nodi del cluster.

Disinstallazione di GFI MailEssentials in un ambiente cluster

Assicurarsi che solo un nodo del cluster sia attivo, il resto deve essere disattivato.

1. Arrestare tutti i servizi di GFI.

2. Eseguire il backup di tutti i contenuti della cartella di installazione di GFI MailEssentials in un percorso diverso.

3. Eliminare tutti i servizi GFI dalle risorse cluster del gruppo GFI MailEssentials.

4. Avviare tutti i servizi GFI e assicurarsi che tutti i servizi cluster e di Exchange siano operativi.

5. Disinstallare dal primo nodo.

6. Aprire l'applet Servizi per assicurare che tutti i servizi di GFI MailEssentialssiano stati eliminati. Per ogni servizio ancora presente nell'applet Servizi, eseguire il seguente comando nel prompt dei comandi: `sc delete <Nome servizio>`. Ad esempio, eseguire `sc delete gfiasmsecatt` se GFI MailEssentials Legacy Attendant è ancora presente.

7. Aprire l'editor del registro di sistema ed eliminare la chiave: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\GFI`

8. Copiare il backup di GFI MailEssentials nella posizione in cui è stato installato.

9. Disattivare il nodo corrente e attivare il successivo. Assicurarsi che tutti i servizi cluster, i servizi di Exchange e GFI MailEssentialssiano operativi.

10. Disinstallare GFI MailEssentials.

11. Aprire l'applet Servizi per assicurare che tutti i servizi di GFI MailEssentialssiano stati eliminati. Per ogni servizio ancora presente nell'applet Servizi, eseguire il seguente comando nel prompt dei comandi: `sc delete <Nome servizio>`. Ad esempio, eseguire `sc delete gfiasmsecatt` se GFI MailEssentials Legacy Attendant è ancora presente.

12. Ripetere i passaggi da 7 a 11 per tutti i nodi rimanenti.

13. Eliminare la cartella di installazione di GFI MailEssentials e il relativo backup.
Dall'amministratore del cluster, eliminare tutti i servizi GFI.

3.2.4 Lotus Domino

Informazioni sull'utilizzo di GFI MailEssentials con Lotus Domino.

» Incompatibilità di Lotus Domino

» Informazioni di installazione per Lotus Domino

» Configurazione cartella antispam di Lotus Domino

Incompatibilità di Lotus Domino

I memo/messaggi interni non vengono scansionati

GFI MailEssentials non scansiona i memo/messaggi interni inviati da Lotus Domino, poiché il formato mittente/destinatario di Lotus Domino non è compatibile. Quando i memo/messaggi interni sono passati a GFI MailEssentials, finiscono in coda e non vengono elaborati.

> **NOTA**
> Non far passare i memo/messaggi interni attraverso GFI MailEssentials.

GFI MailEssentials List Server non è compatibile con Lotus Domino

La creazione di newsletter o elenchi di discussione non funzionerà dal dominio interno di Lotus Domino. Questa opzione non deve essere utilizzata. Se viene usata, gli utenti di Lotus Domino non saranno in grado di inviare messaggi all'elenco.

Guida di installazione di GFI MailEssentials per Lotus Domino

Utilizzare le informazioni della presente sezione per installare e configurare Lotus Domino con GFI MailEssentials. Installare GFI MailEssentials in un computer separato rispetto a Lotus Domino, come nell'immagine sottostante.

Figura 4: installazione di GFI MailEssentials in un computer separato diverso da quello di Lotus Domino

Installare GFI MailEssentials eseguendo il file di installazione di GFI MailEssentials e attenendosi alle istruzioni su schermo. Per ulteriori informazioni, fare riferimento a Installazione (pagina 22).

Se GFI MailEssentials è installato in un computer dove è presente Active Directory, si potrebbe visualizzare la casella di dialogo sottostante. Selezionare **Se non si utilizza Active Directory** per installare GFI MailEssentials in modalità SMTP.

Configurare il computer dove GFI MailEssentials è installato per fungere da gateway (detto anche "Smart host" o server "Mail relay") per tutta la posta. In realtà, tutti i messaggi di posta in entrata devono passare attraverso questo computer per essere scansionati, prima del loro inoltro al server della posta per la distribuzione (è il primo a ricevere tutti i messaggi destinati al server di posta).

Lo stesso vale per i messaggi in uscita, il server della posta deve inoltrare tutti i messaggi in uscita al computer gateway affinché siano scansionati prima di essere inviati ai destinatari esterni tramite Internet (deve essere l'ultima interruzione per i messaggi destinati a Internet). In questo modo, GFI MailEssentials controlla che tutta la posta in entrata e in uscita sia consegnata ai destinatari.

Il record MX del dominio deve indirizzare al relay server della posta

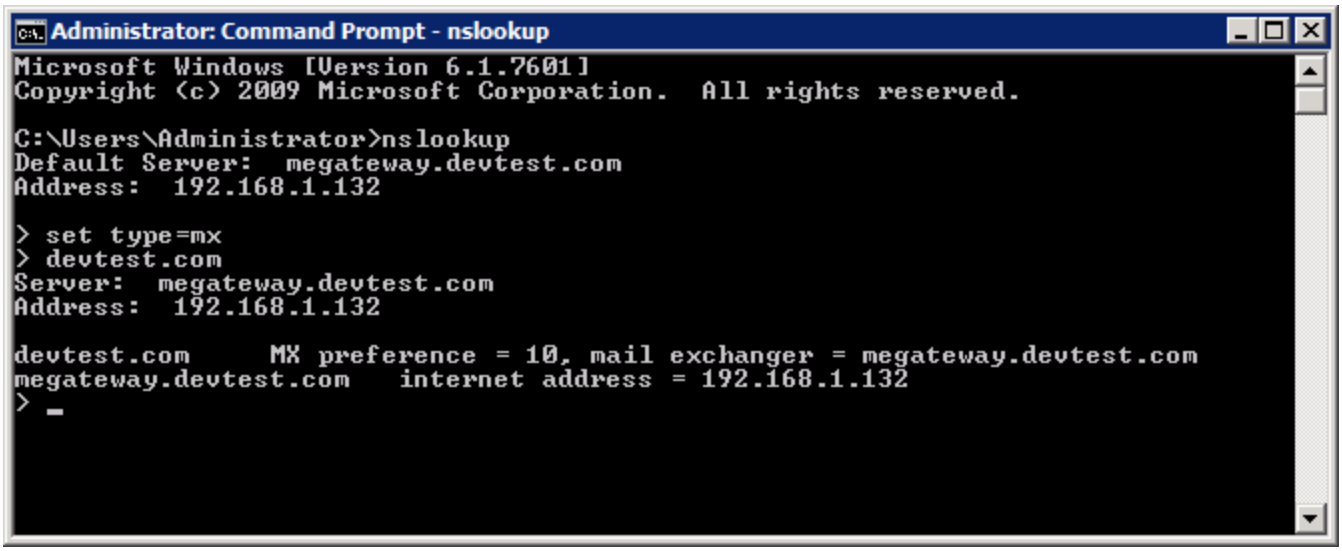
> **NOTA**
> Se l'ISP gestisce il server DNS, chiedere al provider di aggiornarlo.

Dato che il nuovo server di relay deve prima ricevere tutta la posta in entrata, aggiornare il record MX del dominio affinché indirizzi all'IP del nuovo server di relay/gateway della posta.

Verificare che il record MX del server DNS sia il seguente:

1. Dal prompt dei comandi digitare `nslookup` e premere **Invio**.
2. Digitare `set type=mx` e premere **Invio**.
3. Digitare il dominio della posta, quindi premere **Invio**.

Il record MX deve restituire un singolo IP che corrisponde all'indirizzo IP del computer ch esegue GFI MailEssentials.



Schermata 1: verifica del record MX del DNS

4. Verificare il nuovo relay server della posta. Prima di procedere con l'installazione di GFI MailEssentials, verificare che il nuovo relay server della posta funzioni correttamente.

5. Verificare la connessione in entrata SMTP IIS del server relay della posta inviando un messaggio dall'account esterno a un utente interno (utilizzare la web mail, ad esempio **mail.live.com**, se non si dispone di un account esterno). Verificare che il client di posta abbia ricevuto il messaggio.

6. Verificare la connessione SMTP IIS in uscita del server relay della posta inviando un messaggio a un account esterno da un client di posta elettronica. Verificare che l'utente esterno abbia ricevuto il messaggio.

> **NOTA**
> In alternativa, al posto del client di posta elettronica, utilizzare Telnet per l'invio del messaggio. In tal modo, si otterranno più informazioni per la risoluzione dei problemi.

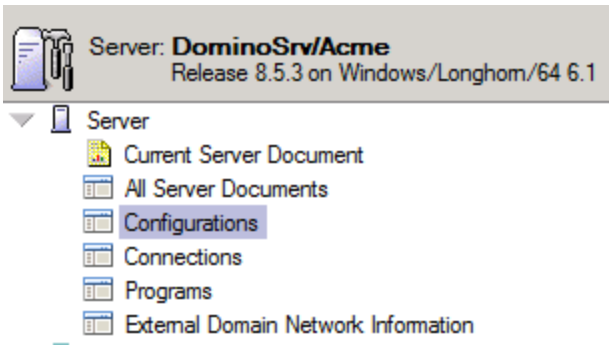
Per ulteriori informazioni, fare riferimento a:

http://support.microsoft.com/support/kb/articles/Q153/1/19.asp

Configurazione di Lotus Domino per l'invio di messaggi in uscita tramite GFI MailEssentials

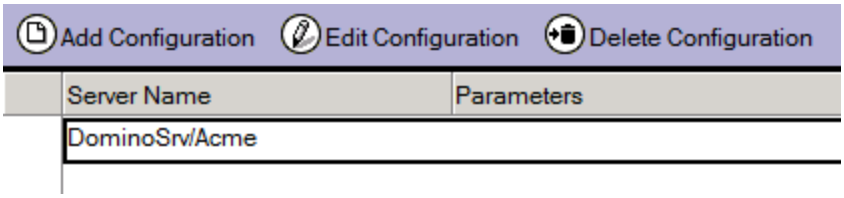
Per indirizzare tutti i messaggi in uscita al server dove è installato GFI MailEssentials, Lotus Domino deve essere configurato come di seguito illustrato.

1. Da IBM Domino Administrator, fare clic sulla scheda **Configuration (Configurazione)** e selezionare **Server > Configurations (Configurazioni)**.



Schermata 2: Lotus Domino Administrator - fare clic sull'opzione Configurations (Configurazioni).

2. Una volta selezionata la sezione di configurazione, la finestra principale mostrerà la configurazione del server. Selezionare il server desiderato, quindi fare clic su **Edit Configuration (Modifica configurazione)**.

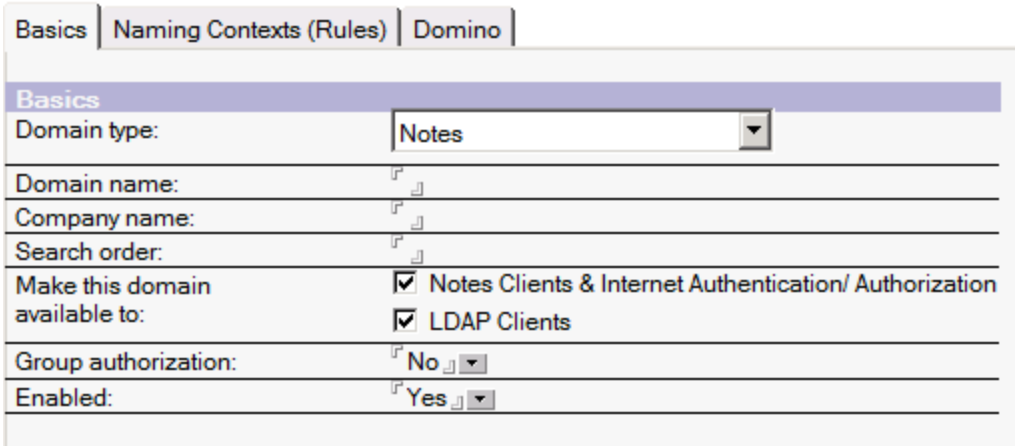


Schermata 3: Fare clic su Edit Configuration (Modifica configurazione).

Dalla pagina del documento di configurazione, selezionare la scheda **Router/SMTP** e assicurarsi che sia selezionata l'opzione **Basics (Operazioni di base)**. Per abilitare la modalità di modifica, fare doppio clic sul contenuto. Selezionare **Relay host for messages leaving the local internet domain (Host di relay per i messaggi che escono dal dominio internet locale)** e immettere l'indirizzo IP del computer che ha installato GFI MailEssentials. Per salvare il documento di configurazione, fare clic su **Save and Close (Salva e chiudi)**.

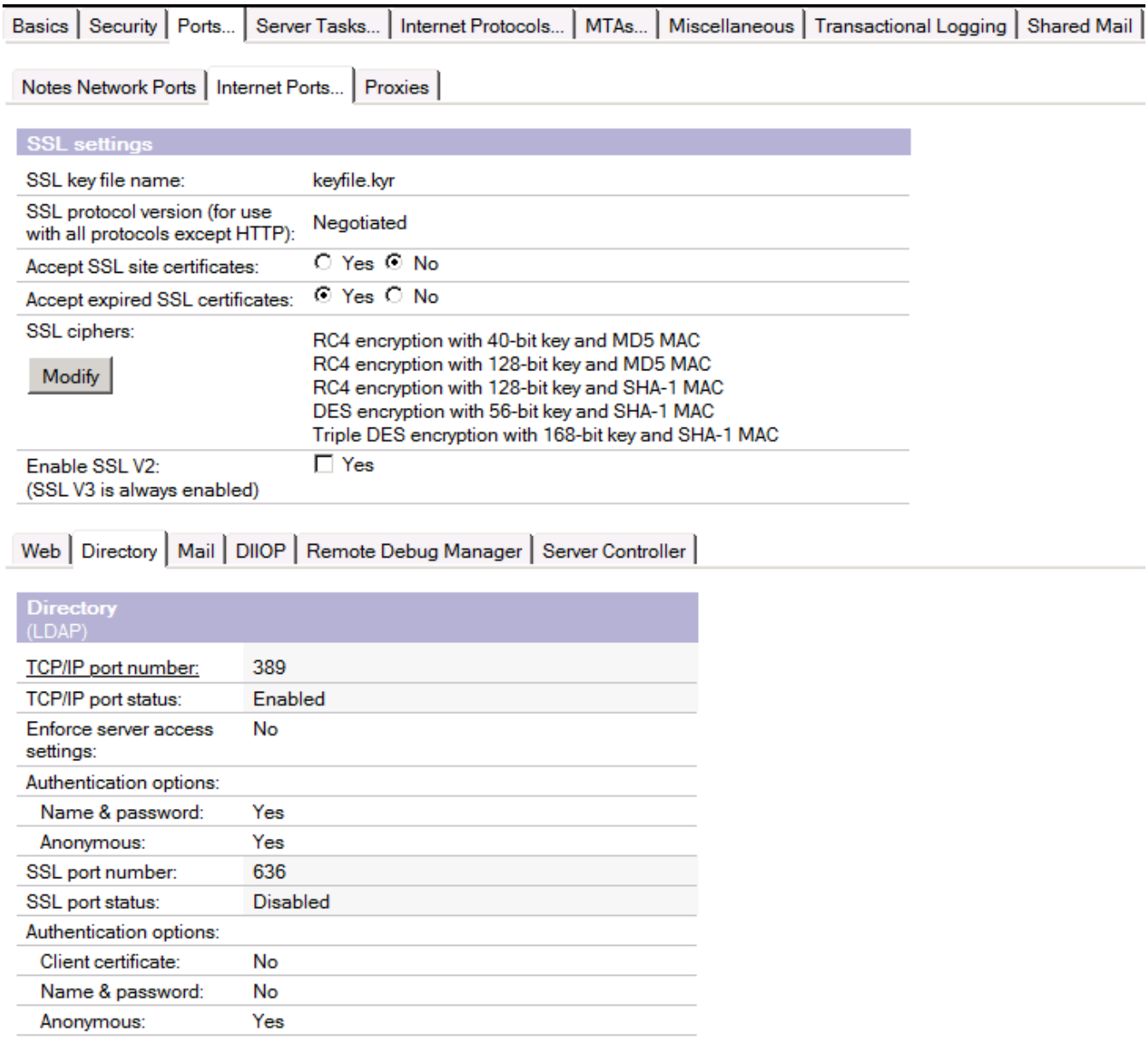
Impostazioni LDAP di Lotus Domino

Da Lotus Domino, abilitare Directory Catalog (Catalogo directory) e Directory Assistance (Assistenza directory). Nel database Directory Assistance (Assistenza directory), fare clic su **Add Directory Assistance (Aggiungi assistenza directory)** per creare un nuovo documento di Assistance (Assistenza). Nel documento, abilitare i client LDAP posti sotto **Make this domain available to (Rendi il dominio disponibile a)** come segue:



Schermata 4: impostazioni LDAP di Lotus Domino

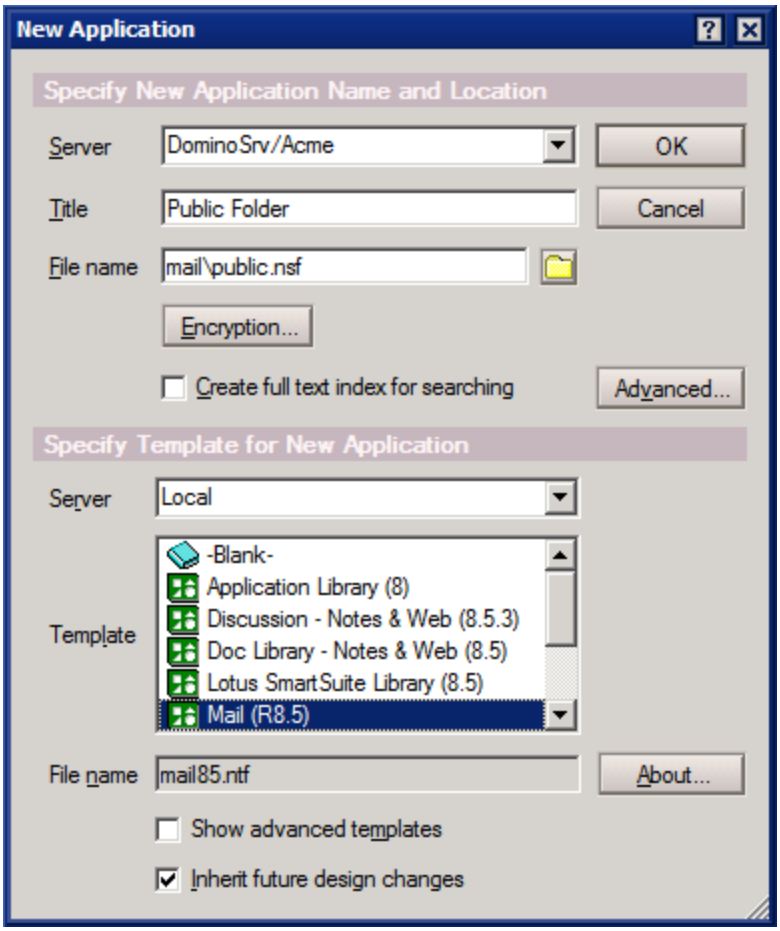
Nella configurazione del server, è necessario modificare le credenziali presenti nella configurazione. È necessario abilitare l'autenticazione anonima per consentire a GFI MailEssentials di accedere a Lotus Domino LDAP.



Schermata 5: abilitazione autenticazione proxy anonima

Configurazione cartella antispam di Lotus Domino

1. Da Lotus Notes Administrator, creare un database con il modello normale MAIL85.NTF, che viene usato come cartella pubblica. Una volta creato il database, fare clic con il pulsante destro del mouse sulla sezione file e selezionare **Access Control (Controllo di accesso)**. Configurare l'utente o il gruppo o il server a cui accedere dal database.



Schermata 6: Creazione di un nuovo database

2. Convertire il database utilizzando la console del server e digitando:

```
load convert -e -h mail\public.nsf
```

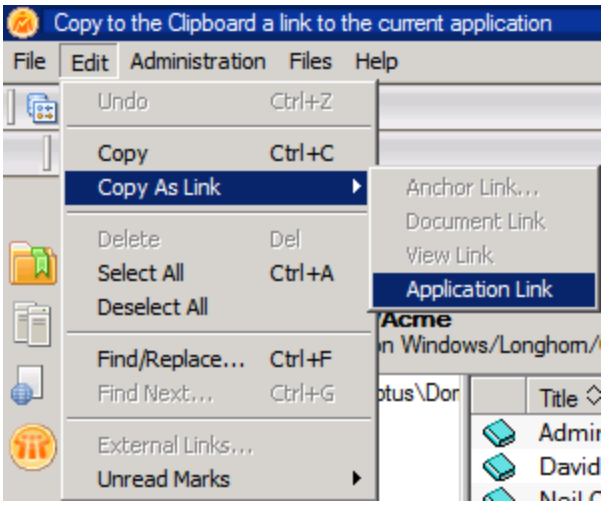
Il comando deve visualizzare i risultati seguenti.

```
load convert -e -h mail\public.nsf

[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Conversion Utility starting
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Convert: Started enabling NSF support for IMAP
in 'mail\public.nsf'
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Convert: Finished enabling NSF support for IMAP
in 'mail\public.nsf'
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Convert: Started adding IMAP specific items in
'mail\public.nsf'
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Convert: Finished adding IMAP specific items in
'mail\public.nsf'. 0 messages succeeded, 0 messages failed.
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Conversion Utility shutdown
```

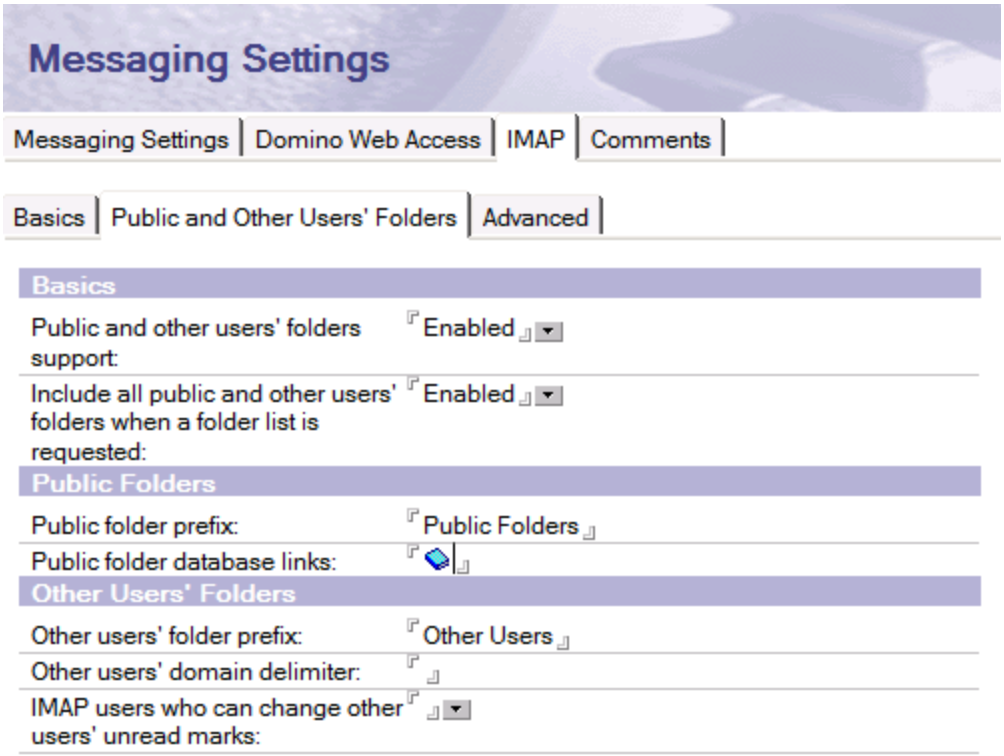
Schermata 7: Caricamento risultati conversione

3. Al completamento, assicurarsi che il database sia accessibile dal servizio IMAP. Da Lotus Notes Administrator, selezionare **Configuration (Configurazione)** e fare clic sulla scheda **Files (File)**. Evidenziare il database della cartella pubblica, fare clic su **Edit (Modifica)**, selezionare **Copy as Link (Copia come collegamento)** e fare clic su **Application Link (Collegamento applicazione)**.



Schermata 8: Copia negli appunti di un collegamento all'applicazione corrente

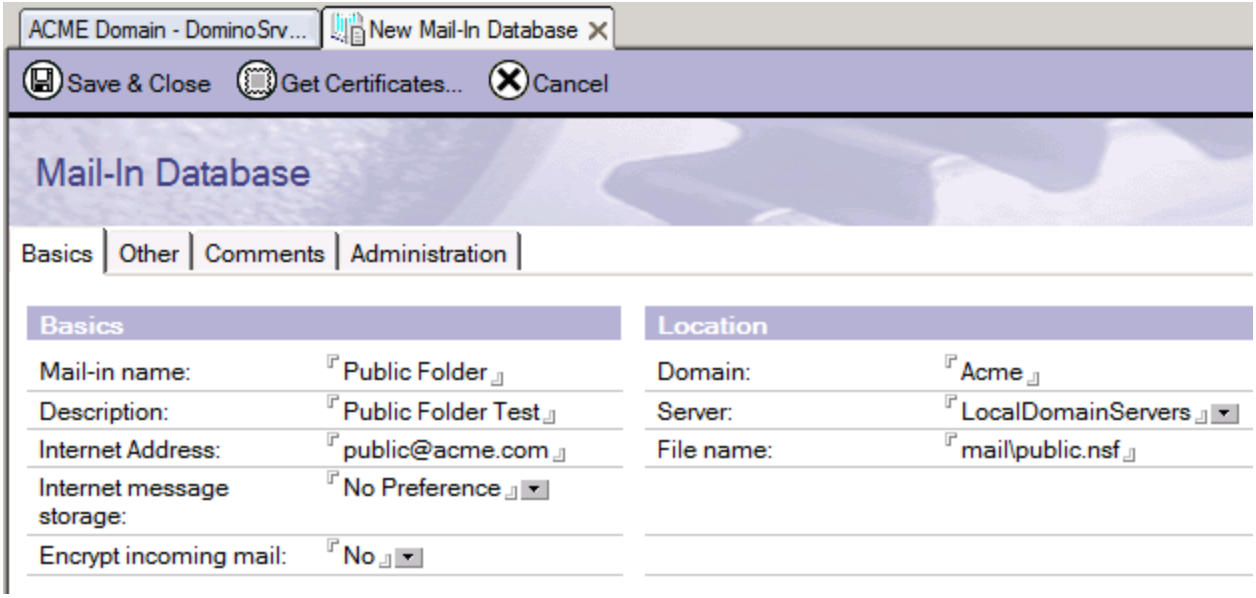
4. Dalla configurazione, selezionare **Messaging Settings (Impostazioni di messaggistica)** e fare clic sulla scheda **IMAP**.



Schermata 9: Includere tutte le cartelle pubbliche e degli altri utenti, quando viene richiesto l'elenco cartelle

5. Selezionare la scheda **Public and Other Users'Folders (Cartelle pubbliche e di altri utenti)**. Fare clic con il pulsante destro del mouse e incollare sopra **Public Folders Database Links (Collegamenti al database cartelle pubbliche)** quindi abilitare **Include all public and other users folders when a folder list is requested (Includi tutte le cartelle pubbliche e degli altri utenti alla richiesta di un elenco cartelle)'**.

6. Salvare e chiudere il documento.



Schermata 10: Nuovo mail-in database

7. Da Lotus Notes Administrator, configurare la cartella per l'utilizzo della posta. Andare a **People and Groups (Persone e gruppi)** e selezionare **Mail-In Database**. Creare un nuovo mail-in database e nel percorso di directory inserire quello completo (ad esempio, Mail\public.nsf).

8. Salvare e chiudere il documento.

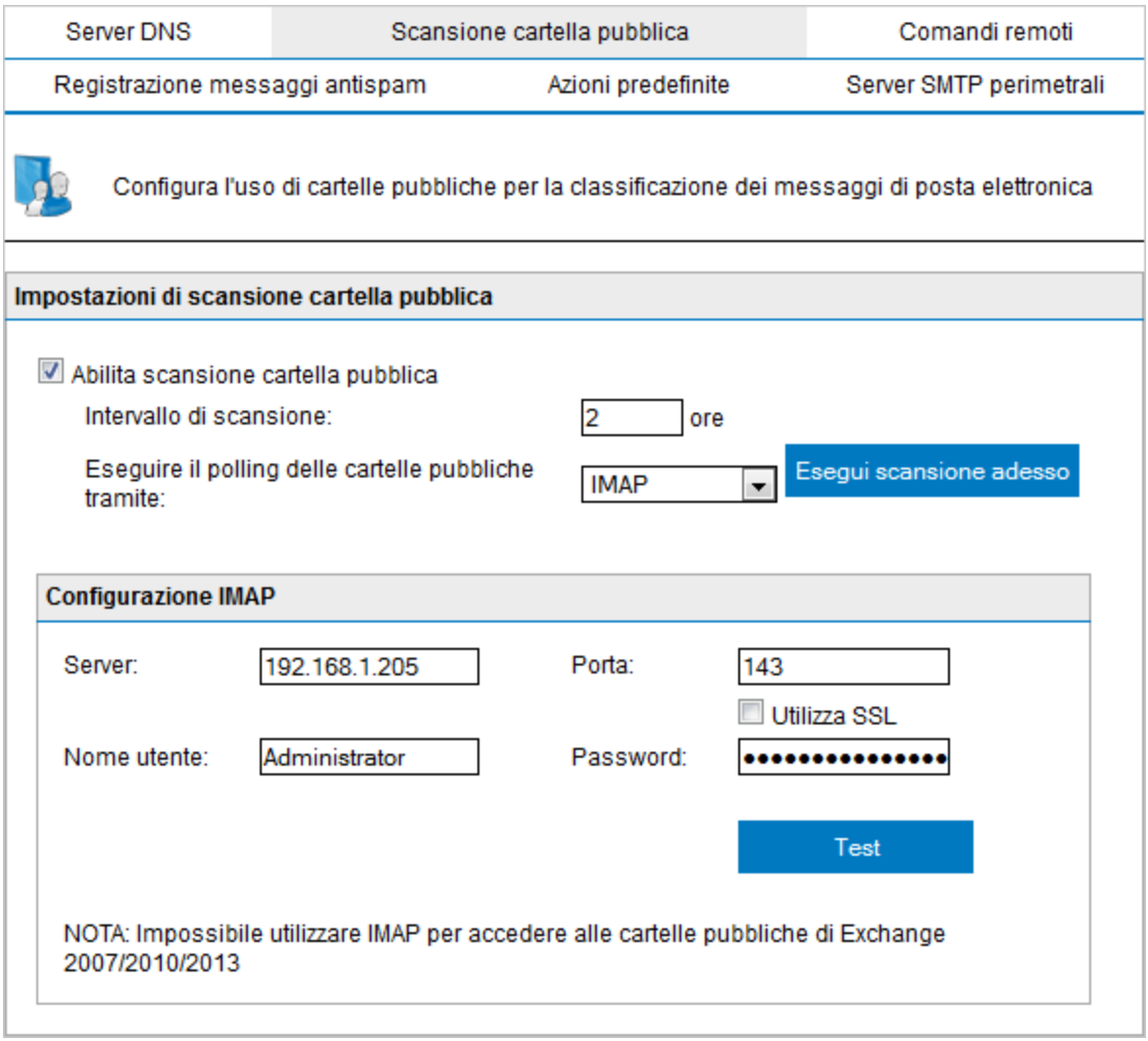
9. Dall'interfaccia web di GFI MailEssentials, espandere **AntiSpam** e selezionare **Impostazioni antispam**.

10. Sul riquadro di destra, selezionare la scheda **Scansione cartella pubblica** e abilitare **Scansione cartella pubblica**.

11. Dalla sezione **Configurazione IMAP**, immettere il server IMAP (il server Lotus Domino, la porta e le credenziali dell'utente per l'accesso alla cartella).

> **NOTA**
> Il pulsante di test non sarà attivo.

12. Fare clic su **Applica** per salvare le modifiche.



Schermata 11: Abilitazione scansione cartella pubblica

13. Dal registro, modificare i valori per consentire l'utilizzo della funzione. Dal registro, selezionare `HKEY_LOCAL_MACHINE\SOFTWARE\GFI\ME12\ATTENDANT\RPFOLDERS:5` e creare i seguenti valori stringa chiave:

```
Name/Value
SharedNamespace Public Folders\\Public Folder
FolderDelimiter \\
```

3.3 Procedura di installazione

La sezione seguente illustra come eseguire l'installazione di GFI MailEssentials.

3.3.1 Note importanti

1. Se si sta attualmente utilizzando una versione precedente di GFI MailEssentials, è possibile aggiornare l'installazione corrente mantenendo al contempo tutte le impostazioni di configurazione esistenti. L'aggiornamento non è reversibile, non è possibile eseguire il downgrade alla versione installata in precedenza.Per ulteriori informazioni, fare riferimento a Aggiornamento da una versione precedente (pagina 48).

2. Se si dispone di SMA e si desidera effettuare l'aggiornamento, accedere all'area clienti del sito web di GFI per aggiornare il codice di licenza attuale.

> **NOTA**
> 'Valutazione' non viene più accettata come codice di licenza. Prima di avviare la procedura di aggiornamento, accedere all'area clienti del sito web di GFI per aggiornare il codice di licenza.

3. Scaricare la build di GFI MailEssentials appropriata per il computer. Utilizzare l'installazione di GFI MailEssentials a 32 bit (x86) per sistemi a 32 bit e quella a 64 bit (x64) per i sistemi a 64 bit.

4. Prima di eseguire la procedura guidata di installazione, assicurarsi:

» di aver effettuato l'accesso con un account con privilegi amministrativi.

» Il computer dove verrà installato GFI MailEssentials risponde ai requisiti di sistema indicati. Per ulteriori informazioni, fare riferimento a Requisiti di sistema (pagina 22).

» Configurare il firewall in uso per consentire a GFI MailEssentials di connettersi ai server GFI. Per ulteriori informazioni, fare riferimento a Impostazioni delle porte del firewall (pagina 25).

» Disabilitare nel software antivirus e di backup di terze parti la scansione delle cartelle utilizzate da GFI MailEssentials. Per ulteriori informazioni, fare riferimento a Software antivirus e di backup (pagina 24).

» Se si installa GFI MailEssentials su un gateway di posta o un relay server/server perimetrale, configurare il computer in questione affinché possa essere utilizzato come gateway.Per ulteriori informazioni, fare riferimento a Installazione in un gateway di posta o su un relay server/server perimetrale (pagina 26).

» Salvare i lavori in sospeso e chiudere tutte le applicazioni aperte nel computer.

6. L'installazione di GFI MailEssentials riavvia i servizi SMTP di Microsoft® Exchange o Microsoft IIS®. Tale operazione è obbligatoria per registrare correttamente i componenti di GFI MailEssentials. Si consiglia di installare GFI MailEssentials in un momento in cui il riavvio di questi servizi non colpisce eccessivamente la rete.

3.3.2 Esecuzione della procedura guidata di installazione

1. Lanciare il programma di installazione di GFI MailEssentials.

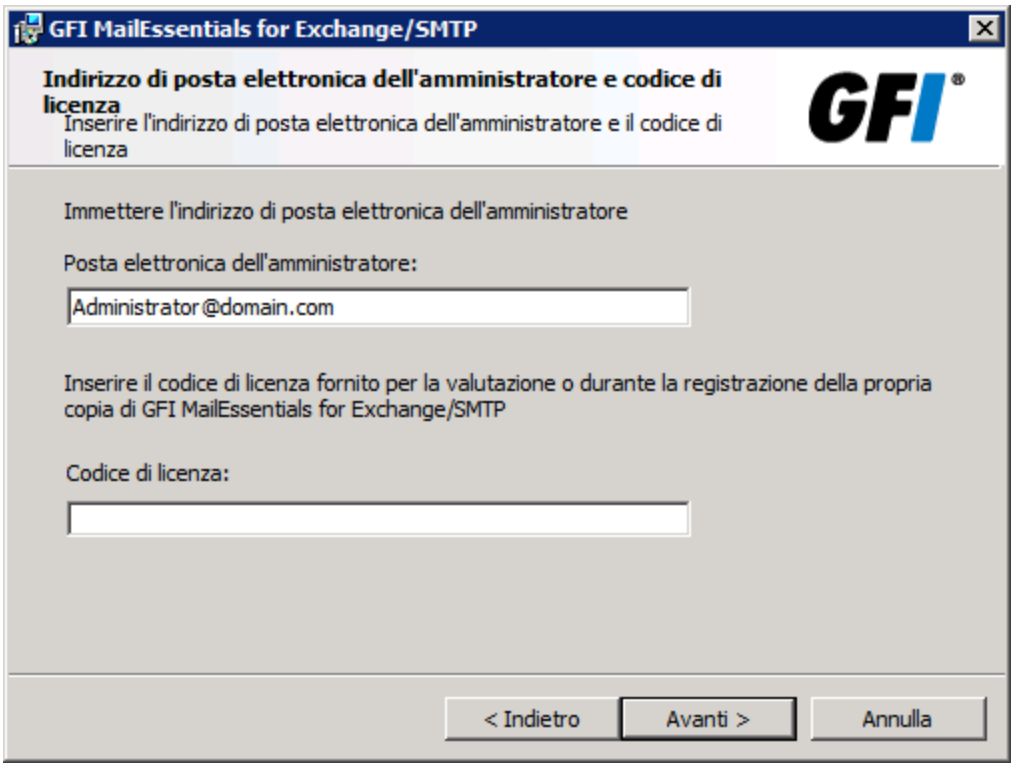
2. Selezionare la lingua da utilizzare con la presente installazione di GFI MailEssentials, quindi fare clic su **Installa**.

> **NOTA**
> La scelta della lingua non è reversibile. Per modificare la lingua selezionata in questa fase, sarà necessario reinstallare GFI MailEssentials.

3. Nella pagina di **Benvenuto**, fare clic su **Avanti**.

4. Selezionare se cercare la presenza di versioni/build più recenti di GFI MailEssentials, quindi fare clic su **Avanti**.

5. Leggere il contratto di licenza e, se d'accordo con i termini e le condizioni riportate in esso, selezionare **Accetto i termini del contratto di licenza**. Fare clic su **Avanti**.


GFI MailEssentials for Exchange/SMTP
Indirizzo di posta elettronica dell'amministratore e codice di licenza
Inserire l'indirizzo di posta elettronica dell'amministratore e il codice di licenza
Immettere l'indirizzo di posta elettronica dell'amministratore
Posta elettronica dell'amministratore:
Administrator@domain.com
Inserire il codice di licenza fornito per la valutazione o durante la registrazione della propria copia di GFI MailEssentials for Exchange/SMTP
Codice di licenza:
< Indietro
Avanti >
Annulla

Schermata 12: Inserimento dell'indirizzo di posta elettronica dell'amministratore e del codice di licenza

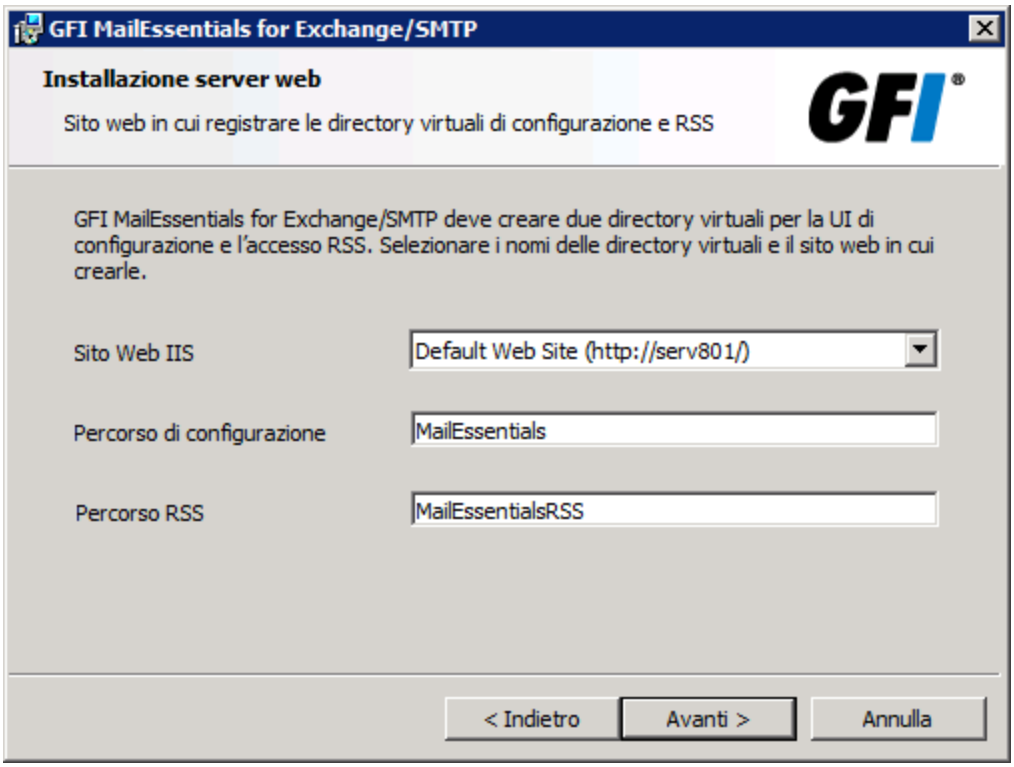
6. Digitare l'indirizzo di posta elettronica dell'amministratore in **Indirizzo e-mail amministratore**, quindi compilare l'area **Codice di licenza**. Fare clic su **Avanti**.

> **NOTA**
> 'Valutazione' non viene più accettata come codice di licenza. Prima di avviare la procedura di aggiornamento, accedere all'area clienti del sito web di GFI per aggiornare il codice di licenza.

7. Selezionare la modalità che verrà utilizzata da GFI MailEssentials per recuperare l'elenco di utenti della posta.

Opzione	Descrizione
Sì, tutti gli utenti di posta elettronica sono disponibili su Active Directory. Le regole verranno create in base agli utenti di Active Directory.	**Modalità Active Directory** GFI MailEssentials recupererà l'elenco degli utenti da Active Directory. La scelta di questa opzione indica che GFI MailEssentials viene installato dietro il firewall e che ha accesso alla Active Directory contenente TUTTI gli utenti della posta.
No, non sono provvisto di Active Directory o la mia rete non ha accesso ad Active Directory (DMZ)	**Modalità SMTP** Selezionare questa modalità se si installa GFI MailEssentials in un computer che non dispone di accesso alla Active Directory contenente l'elenco completo di tutti gli utenti di posta. Questo include i computer in una DMZ o che non fanno parte di un dominio Active Directory. In questa modalità, GFI MailEssentials popola automaticamente l'elenco di utenti locali utilizzando l'indirizzo di posta del mittente nei messaggi in uscita. Il presente elenco di utenti può essere gestito anche dal nodo di Impostazioni generali di GFI MailEssentials. Per ulteriori informazioni, fare riferimento a Gestione utenti locali (pagina 245).

Fare clic su **Avanti**.


GFI MailEssentials for Exchange/SMTP
Installazione server web
Sito web in cui registrare le directory virtuali di configurazione e RSS
GFI
GFI MailEssentials for Exchange/SMTP deve creare due directory virtuali per la UI di configurazione e l'accesso RSS. Selezionare i nomi delle directory virtuali e il sito web in cui crearle.
Sito Web IIS
Default Web Site (http://serv801/)
Percorso di configurazione
MailEssentials
Percorso RSS
MailEssentialsRSS
< Indietro
Avanti >
Annulla

Schermata 13: Dati server SMTP e directory virtuale

8. Nella finestra di dialogo **Installazione server web**, impostare le seguenti opzioni:

> **NOTA**
> Di norma, le impostazioni predefinite sono corrette per la maggioranza delle installazioni.

Opzione	Descrizione
sito web in cui creare la directory virtuale di GFI MailEssentials	Selezionare il sito web dove ospitare le directory virtuali di GFI MailEssentials.
La directory virtuale di GFI MailEssentials Configuration	Indicare un nome per la directory virtuale di GFI MailEssentials.
La directory virtuale dei feed RSS quarantena di GFI MailEssentials	Indicare un nome per la directory virtuale dei feed RSS quarantena di GFI MailEssentials.
Installazione server SMTP	Selezionare il server SMTP a cui GFI MailEssentials si associa. Per impostazione predefinita, GFI MailEssentials si associa al server virtuale SMTP predefinito. Se nel dominio sono presenti più server SMTP virtuali, è possibile associare GFI MailEssentials a qualsiasi server SMTP virtuale disponibile. **NOTE** 1. Se si installa in un computer con Microsoft® Exchange Server 2007/2010/2013, questa opzione non viene visualizzata poiché Microsoft® Exchange dispone già di server SMTP integrato. 2. Dopo l'installazione, è sempre possibile associare GFI MailEssentials a un altro server SMTP virtuale da GFI MailEssentials Configuration. Per ulteriori informazioni, fare riferimento a Binding server virtuale SMTP (pagina 246).

Fare clic su **Avanti**.

9. Selezionare la cartella in cui installare GFI MailEssentials e fare clic su **Avanti**. Quando l'installazione è un aggiornamento, GFI MailEssentials si installa nel medesimo percorso dell'installazione precedente.

10. Per avviare la procedura di installazione, fare clic su **Installa**. Se viene richiesto di riavviare i servizi SMTP, fare clic su **Sì**.

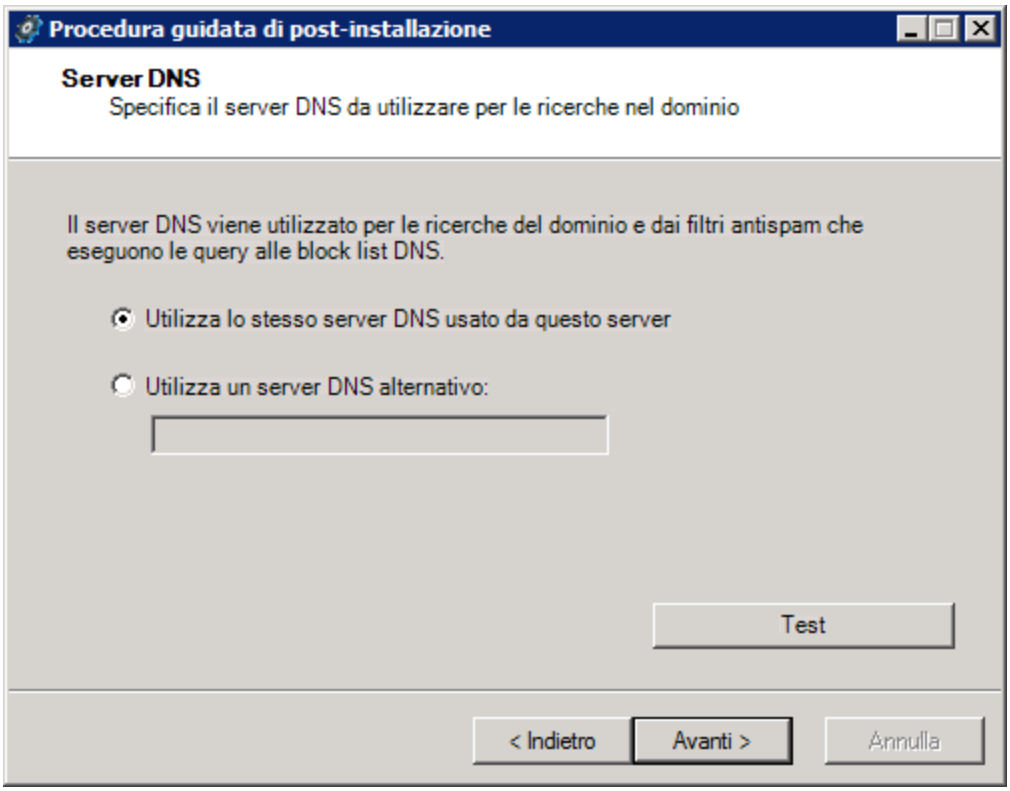
11. Al termine, fare clic su **Fine**.

> **NOTA**
> Per le nuove installazioni, la configurazione avvierà automaticamente la Procedura guidata di post-installazione. Per ulteriori informazioni, fare riferimento a Procedura guidata di post-installazione (pagina 44).

3.3.3 Procedura guidata di post-installazione

La procedura guidata di post-installazione viene caricata automaticamente dopo la prima installazione di GFI MailEssentials. Consente la configurazione delle impostazioni più importanti di GFI MailEssentials.

1. Fare clic su **Avanti** nella pagina di benvenuto.

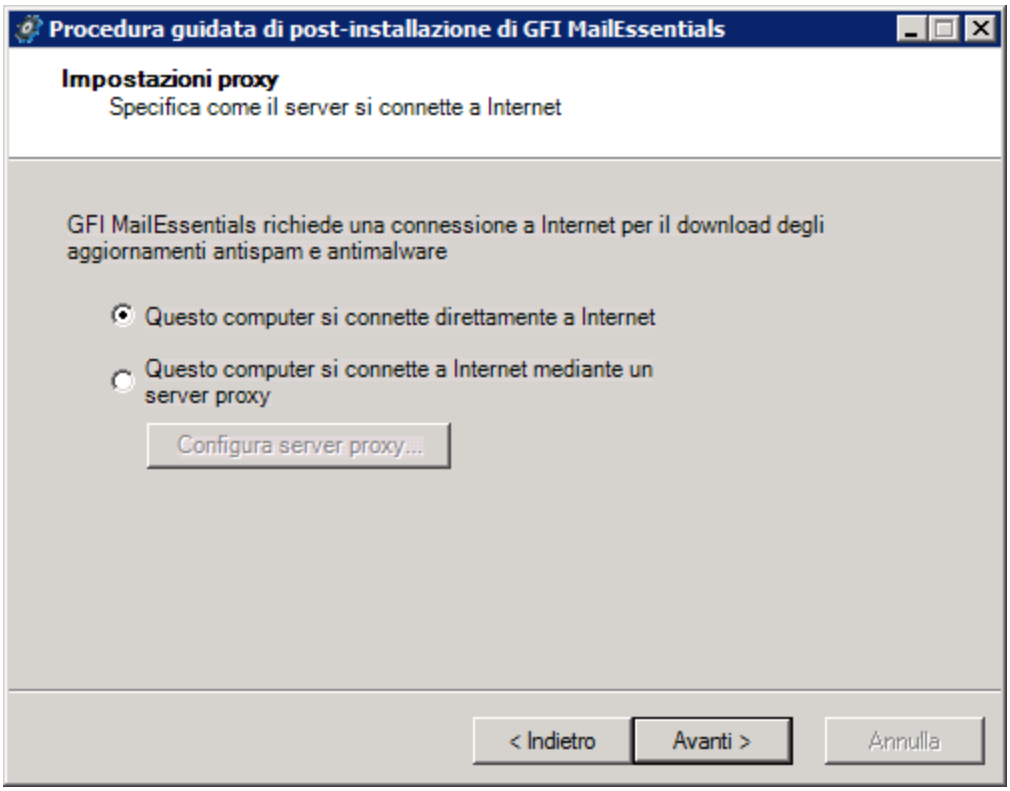

Procedura guidata di post-installazione
Server DNS
Specifica il server DNS da utilizzare per le ricerche nel dominio
Il server DNS viene utilizzato per le ricerche del dominio e dai filtri antispam che eseguono le query alle block list DNS.
Utilizza lo stesso server DNS usato da questo server
Utilizza un server DNS alternativo:
Test
< Indietro
Avanti >
Annulla

Schermata 14: impostazioni server DNS

2. Nella finestra di dialogo Server DNS, selezionare:

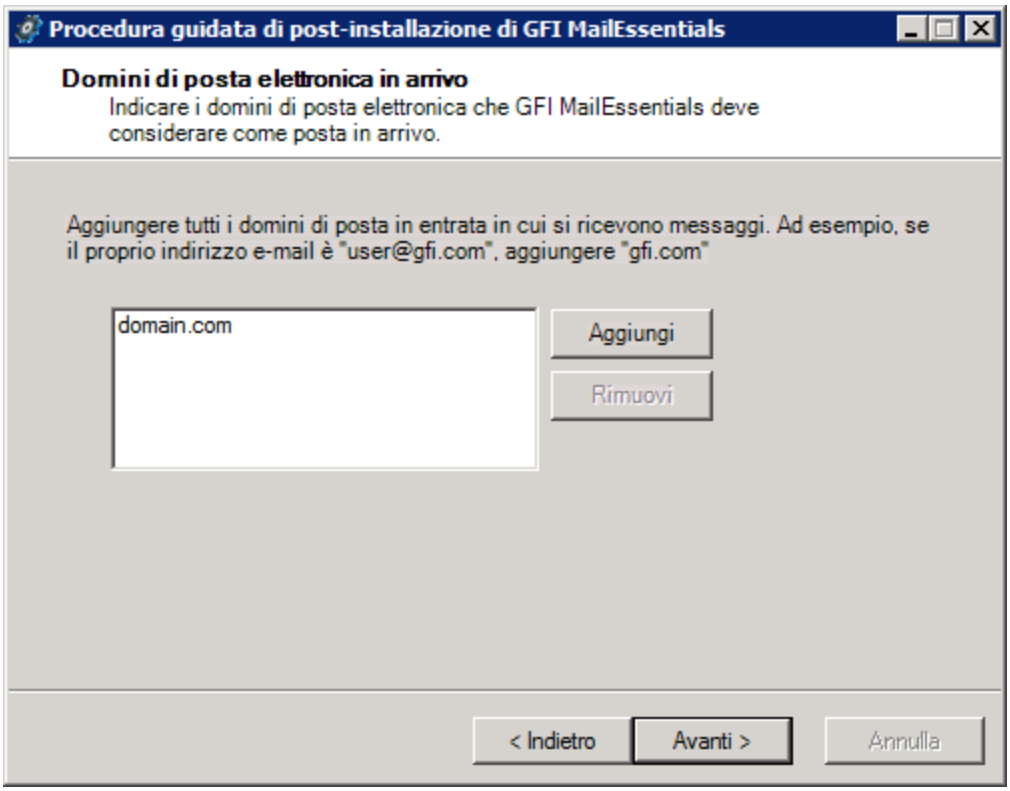
Opzione	Descrizione
Utilizza lo stesso server DNS usato da questo server	Selezionare questa opzione per utilizzare lo stesso server DNS utilizzato dal sistema operativo dove è installato GFI MailEssentials.
Utilizza un server DNS alternativo	Selezionare questa opzione per specificare un indirizzo IP personalizzato del server DNS.

Fare clic su **Test** per provare la connessione con il server DNS specificato. Se la verifica ha esito negativo, specificare un altro server DNS. Fare clic su **Avanti**.


Procedura guidata di post-installazione di GFI MailEssentials
Impostazioni proxy
Specifica come il server si connette a Internet
GFI MailEssentials richiede una connessione a Internet per il download degli aggiornamenti antispam e antimalware
Questo computer si connette direttamente a Internet
Questo computer si connette a Internet mediante un server proxy
Configura server proxy...
< Indietro
Avanti >
Annulla

Schermata 15: impostazioni proxy

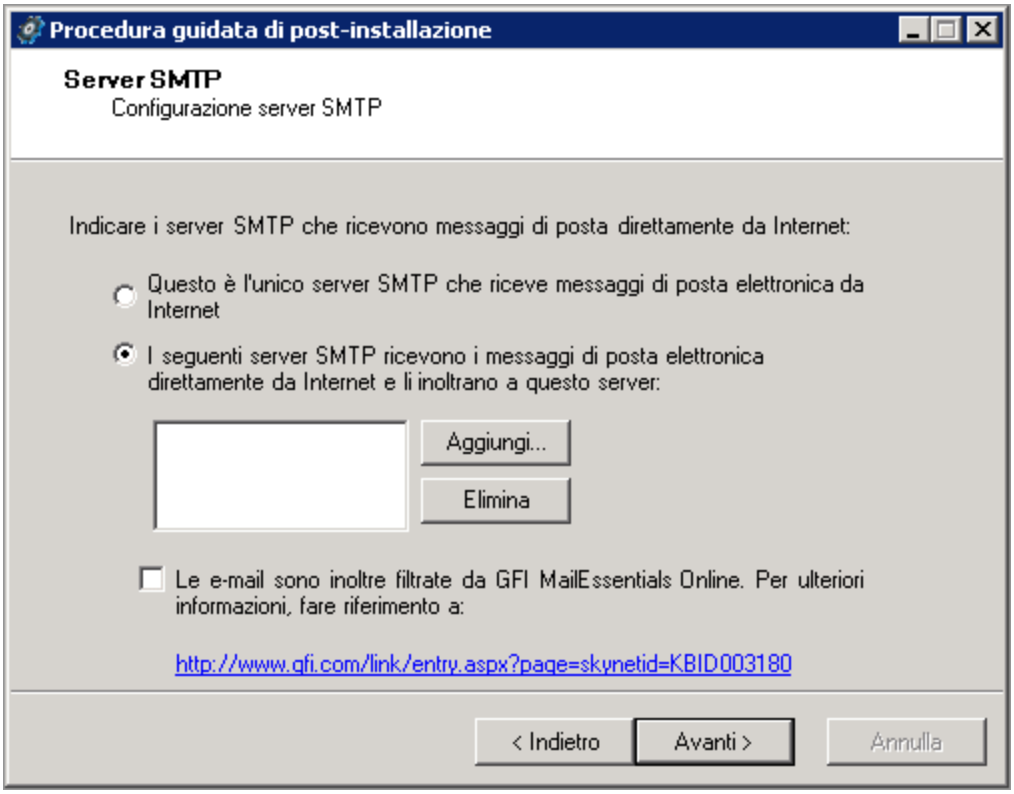
3. Nella finestra di dialogo **Impostazioni proxy**, indicare la modalità con cui GFI MailEssentials si connette a Internet. Se il server si connette tramite server proxy, fare clic su **Configura server proxy…** e specificare le impostazioni proxy. Fare clic su **Avanti**.


Procedura guidata di post-installazione di GFI MailEssentials
Domini di posta elettronica in arrivo
Indicare i domini di posta elettronica che GFI MailEssentials deve considerare come posta in arrivo.
Aggiungere tutti i domini di posta in entrata in cui si ricevono messaggi. Ad esempio, se il proprio indirizzo e-mail è "user@gfi.com", aggiungere "gfi.com"
domain.com
Aggiungi
Rimuovi
< Indietro
Avanti >
Annulla

Schermata 16: Domini di posta elettronica in arrivo

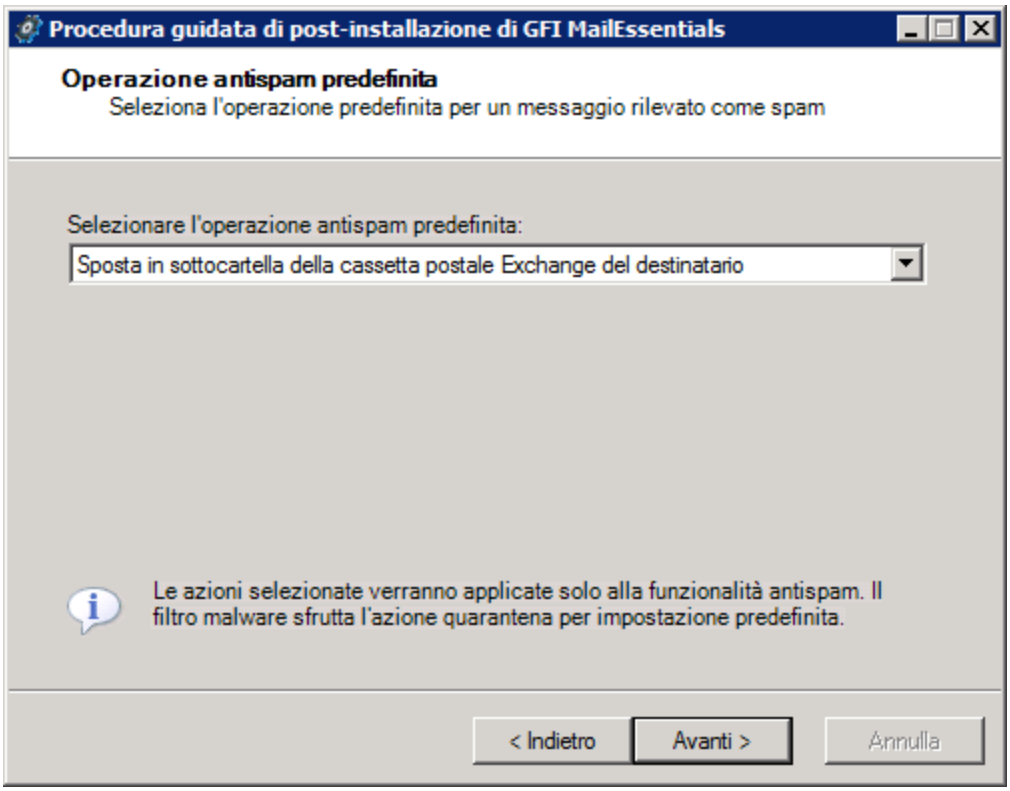
4. Nella finestra di dialogo **Domini di posta elettronica in arrivo**, specificare tutti i domini da scansionare alla ricerca di virus e spam. Tutti i domini locali che non sono specificati nell'elenco non verranno scansionati. Fare clic su **Avanti**.

> **NOTA**
> Al momento di aggiungere i domini, selezionare **Ottieni record MX del dominio e includi nell'elenco dei server perimetrali** per recuperare i record MX del dominio e aggiungerli automaticamente all'elenco dei server SMTP perimetrali (configurato nel passaggio successivo).


Procedura guidata di post-installazione
Server SMTP
Configurazione server SMTP
Indicare i server SMTP che ricevono messaggi di posta direttamente da Internet:
Questo è l'unico server SMTP che riceve messaggi di posta elettronica da Internet
I seguenti server SMTP ricevono i messaggi di posta elettronica direttamente da Internet e li inoltrano a questo server:
Aggiungi...
Elimina
Le e-mail sono inoltre filtrate da GFI MailEssentials Online. Per ulteriori informazioni, fare riferimento a:
http://www.gfi.com/link/entry.aspx?page=skynetid=KBID003180
< Indietro
Avanti >
Annulla

Schermata 17: impostazioni server SMTP

5. Nella finestra di dialogo **Server SMTP**, specificare in che modo il server riceve la posta esterna. Se la posta viene instradata attraverso altri server prima dell'inoltro al server GFI MailEssentials, aggiungere l'indirizzo IP degli altri server nell'elenco. Per maggiori informazioni sui server SMTP perimetrali, consultare: http://go.gfi.com/?pageid=ME_PerimeterServer. Se si utilizza il prodotto di sicurezza e-mail in hosting GFI MailEssentials Online, abilitare la casella di controllo **I messaggi di posta elettronica vengono anche filtrati da…**. Per maggiori informazioni, consultare: http://go.gfi.com/?pageid=ME_MAXMPME. Fare clic su **Avanti**.


Procedura guidata di post-installazione di GFI MailEssentials
Operazione antispam predefinita
Seleziona l'operazione predefinita per un messaggio rilevato come spam
Selezionare l'operazione antispam predefinita:
Sposta in sottocartella della cassetta postale Exchange del destinatario
Le azioni selezionate verranno applicate solo alla funzionalità antispam. Il filtro malware sfrutta l'azione quarantena per impostazione predefinita.
< Indietro
Avanti >
Annulla

Schermata 18: scelta dell'operazione antispam predefinita da effettuare

6. Nella finestra di dialogo **Operazione antispam predefinita**, selezionare l'operazione predefinita da eseguire al rilevamento di un messaggio spam. Questa operazione verrà applicata solo ai filtri antispam. I filtri malware inseriscono automaticamente in quarantena i messaggi bloccati. Per ulteriori informazioni, fare riferimento a Motori di scansione e filtro della posta elettronica (pagina 16).

> **NOTA**
> Se si installa su Microsoft® Exchange 2010 e l'operazione predefinita selezionata è **Sposta in sottocartella della cassetta postale Exchange del destinatario**, è necessario creare un utente con diritti di rappresentazione. Scegliere se consentire a GFI MailEssentials di creare automaticamente l'utente oppure specificare le credenziali manualmente e fare clic su **Imposta diritti di accesso** per assegnare i diritti necessari all'utente specificato. L'utente deve essere dedicato esclusivamente a questa funzionalità e le credenziali non devono essere modificate. Per maggiori informazioni, consultare http://go.gfi.com/?pageid=ME_SpamExch2010.

Fare clic su **Avanti**.

7. Al momento di installare su Microsoft® Exchange Server 2007/2010, viene visualizzato l'elenco dei ruoli server rilevati di Microsoft® Exchange e dei componenti necessari di GFI MailEssentials. Per installare i componenti necessari di GFI MailEssentials, fare clic su **Avanti**.

8. Per finalizzare l'installazione, fare clic su **Fine**.

Adesso l'installazione di GFI MailEssentials è completa e il sistema di protezione della posta è pronto.

Passaggi successivi: Ottimizzare il sistema di protezione per assicurarsi che sia effettivamente operativo. Per ulteriori informazioni, fare riferimento a Azioni post-installazione (pagina 50).

NOTA

Per rieseguire la Procedura guidata di post-installazione, selezionare la cartella di installazione di GFI MailEssentials ed eseguire il seguente comando:

```
e2kwiz.exe clean
```

3.4 Aggiornamento da una versione precedente

Aggiornamento alla versione più recente di GFI MailEssentials da:

» GFI MailEssentials 2012

» GFI MailEssentials 12 e versioni superiori e/o GFI MailSecurity 10.1 e versioni superiori.

Note importanti

1. Prima di eseguire l'aggiornamento alla versione più recente di GFI MailEssentials, assicurarsi che il sistema soddisfi i requisiti minimi. Per ulteriori informazioni, fare riferimento a Requisiti di sistema (pagina 22).

2. L'aggiornamento non è reversibile, non è possibile eseguire il downgrade alla versione installata in precedenza.

3.4.1 Aggiornamento dalla versione 2012 o più recente

Per eseguire l'aggiornamento di GFI MailEssentials 2012 o versioni successive alla versione più recente, avviare il programma di installazione più recente sul server dove è attualmente presente l'installazione di GFI MailEssentials. Dopo aver accettato il Contratto di licenza con l'utente finale, il programma di installazione rileva l'installazione esistente e mostra il percorso di installazione della versione precedente. Per eseguire l'aggiornamento, fare clic su **Avanti** e al termine, selezionare **Fine**.

Per eseguire l'aggiornamento da una versione principale all'altra, è necessario un nuovo codice di licenza, ad esempio, per aggiornare da GFI MailEssentials 2012 a GFI MailEssentials 2014 R2. È possibile richiedere il nuovo codice dall'area clienti di GFI.

Microsoft ® Exchange 2007 e versioni superiori

Per gli aggiornamenti su Microsoft® Exchange 2007 e versioni successive, la procedura di post-installazione viene visualizzata dopo l'installazione. Mostra l'elenco di ruoli server di Microsoft® Exchange che sono stati rilevati, oltre ai componenti necessari per GFI MailEssentials. Per installare i componenti necessari di GFI MailEssentials, fare clic su **Avanti** e quindi su **Fine** per terminare la procedura guidata di post-installazione.

3.4.2 Aggiornamento da versioni precedenti

Informazione sulle modalità di aggiornamento alla versione più recente di GFI MailEssentials da:

» GFI MailEssentials versioni 12, 14, 2010

» GFI MailSecurity versioni 10.1 e 2011

GFI MailEssentials 2012 e 2014 hanno introdotto una serie di cambiamenti nelle funzionalità disponibili nelle versioni di cui sopra. Per ulteriori informazioni, fare riferimento alla Guida all'aggiornamento di GFI MailEssentials. I cambiamenti principali includono:

- Le funzioni antispam e antivirus sono unite in un'unica soluzione
- Nuova interfaccia utente basata sul web
- Presenti differenze nei motori antivirus
- La creazione di rapporti è integrata all'interno dell'interfaccia utente
- Altri aggiornamenti

Scegliere l'ambiente di cui si esegue l'aggiornamento:

- GFI MailEssentials versioni 12, 14, 2010
- GFI MailSecurity versioni 10.1, 2011
- Sia GFI MailEssentials che GFI MailSecurity

Aggiornamento di GFI MailEssentials versioni 12, 14, 2010

Le funzioni antispam e antiphishing sono concesse in licenza al momento dell'aggiornamento. Le funzioni antivirus e antimalware sono disponibili per un periodo di prova di 30 giorni.

Installare GFI MailEssentials come se fosse la prima installazione. Per ulteriori informazioni, fare riferimento a Procedura di installazione (pagina 40).

Per gli aggiornamenti su Microsoft® Exchange 2007 e versioni successive, la procedura di post-installazione viene visualizzata dopo l'installazione. Mostra l'elenco di ruoli server di Microsoft® Exchange che sono stati rilevati, oltre ai componenti necessari per GFI MailEssentials. Per installare i componenti necessari di GFI MailEssentials, fare clic su **Avanti** e quindi su **Fine** per terminare la procedura guidata di post-installazione.

Aggiornamento a GFI MailSecurity versioni 10.1, 2011

Le funzioni antivirus e antimalware sono concesse in licenza al momento dell'aggiornamento. Le funzioni antispam e antiphishing sono disponibili per un periodo di prova di 30 giorni.

Installare GFI MailEssentials come se fosse la prima installazione. Per ulteriori informazioni, fare riferimento a Procedura di installazione (pagina 40).

Dopo l'installazione, completare anche la procedura guidata di post-installazione di GFI MailEssentials. Per ulteriori informazioni, fare riferimento a Procedura guidata di post-installazione (pagina 44).

Aggiornamento sia di GFI MailEssentials che di GFI MailSecurity

Quando si esegue l'aggiornamento di un server che contiene sia GFI MailEssentials che GFI MailSecurity, tutte le funzioni antivirus, antimalware, antispam e antiphishing vengono concesse in licenza al momento dell'aggiornamento.

Installare GFI MailEssentials come se fosse la prima installazione. Per ulteriori informazioni, fare riferimento a Procedura di installazione (pagina 40).

Per gli aggiornamenti su Microsoft® Exchange 2007 e versioni successive, la procedura di post-installazione viene visualizzata dopo l'installazione. Mostra l'elenco di ruoli server di Microsoft® Exchange che sono stati rilevati, oltre ai componenti necessari per GFI MailEssentials. Per installare i componenti necessari di GFI MailEssentials, fare clic su **Avanti** e quindi su **Fine** per terminare la procedura guidata di post-installazione.

3.5 Azioni post-installazione

Per assicurare che il sistema di scansione e di filtro di GFI MailEssentials sia effettivamente operativo, effettuare le seguenti azioni post-installazione:

Tabella 1: Azioni post-installazione

Azione	Descrizione
Aggiungere i motori di scansione di GFI MailEssentials all'elenco di eccezioni di Protezione esecuzione programmi di Windows.	Data Execution Prevention (DEP) rappresenta una serie di tecnologie hardware e software che eseguono controlli della memoria per impedire a codice dannoso di essere eseguito sul sistema. Se GFI MailEssentials è stato installato su un sistema operativo che include DEP, sarà necessario aggiungere gli eseguibili del motore di scansione di GFI MailEssentials (**GFiScanM.exe**) e del motore di scansione antivirus Kaspersky (**kavss.exe**). **NOTA** Questa operazione è obbligatoria solo quando si installa su Microsoft® Windows Server 2003 SP 1 o SP 2. Per ulteriori informazioni, fare riferimento a Aggiunta di motori all'elenco di eccezioni di Protezione esecuzione programmi di Windows (pagina 50).
Avviare GFI MailEssentials Configuration.	Fare clic su **Start > Tutti i programmi >GFI MailEssentials > GFI MailEssentials Configuration**.
Abilitare raccolta di directory	Gli attacchi di Raccolta di directory si verificano quando gli spammer cercano di indovinare gli indirizzi di posta allegando i nomi utente noti al dominio della vittima. La maggioranza degli indirizzi di posta elettronica è inesistente.Questo filtro è abilitato per impostazione predefinita se GFI MailEssentials è installato in un ambiente Active Directory. Per ulteriori informazioni, fare riferimento a Raccolta di directory (pagina 115).
Abilita greylist	Il filtro greylist blocca temporaneamente i messaggi di posta in arrivo ricevuti da mittenti sconosciuti. Normalmente, i sistemi di posta attendibili ritentano l'invio dopo alcuni minuti, gli spammer invece ignorano tali messaggi di errore.Questo filtro non è abilitato per impostazione predefinita. Per ulteriori informazioni, fare riferimento a Greylist (pagina 130).Per ulteriori informazioni, fare riferimento a Greylist (pagina 130).
Configurazione whitelist	La whitelist contiene gli elenchi dei criteri che identificano la posta attendibile. Le e-mail che rispettano tali criteri non saranno scansionate dai filtri antispam e verranno sempre recapitate al destinatario. Per ulteriori informazioni, fare riferimento a Whitelist (pagina 141).
Verifica dell'installazione	Dopo aver configurato tutte le azioni post-installazione, GFI MailEssentials è pronto per iniziare a proteggere e filtrare il sistema di posta da messaggi spam e dannosi. Verificare l'installazione per assicurarsi che GFI MailEssentials funzioni correttamente. Per ulteriori informazioni, fare riferimento a Verifica dell'installazione (pagina 51).

3.5.1 Aggiunta di motori all'elenco di eccezioni di Protezione esecuzione programmi di Windows

Data Execution Prevention (DEP) rappresenta una serie di tecnologie hardware e software che eseguono controlli della memoria per impedire a codice dannoso di essere eseguito sul sistema.

Se GFI MailEssentials è stato installato su un sistema operativo che include DEP, sarà necessario aggiungere gli eseguibili del motore di scansione di GFI MailEssentials (**GFiScanM.exe**) e del motore di scansione antivirus Kaspersky (**kavss.exe**).

NOTA

Questa operazione è obbligatoria solo quando si installa su Microsoft® Windows Server 2003 SP 1 o SP 2.

Per aggiungere gli eseguibili di GFI all'elenco di eccezione di Protezione esecuzione programmi:

1. Da **Pannello di controllo** aprire l'applet **Sistema**.

2. Dalla scheda **Avanzate**, nell'area **Prestazioni**, fare clic su **Impostazioni**.

3. Fare clic sulla scheda **Protezione esecuzione programmi**.

4. Fare clic su **Attiva Protezione esecuzione programmi per tutti i programmi e i servizi tranne quelli selezionati**.

5. Fare clic su **Aggiungi** e, dalla casella della finestra di dialogo, cercare:***<GFI MailEssentials percorso di installazione>**GFI**MailEssentials*\Sicurezza e-mail**, quindi scegliere **GFiScanM.exe**.

6. Fare clic su **Aggiungi** e nella finestra di dialogo passare a: ***<GFI MailEssentials percorso di installazione>**GFI**MailEssentials*\AntiVirus\Kaspersky**, quindi selezionare **kavss.exe**.

7. Per applicare le modifiche, fare clic su **Applica** e su **OK**.

8. Riavviare il servizio **GFI MailEssentials Autoupdater** e i servizi **GFI MailEssentials AV Scan Engine**.

3.5.2 Verifica dell'installazione

Dopo aver configurato tutte le azioni post-installazione, GFI MailEssentials è pronto per iniziare a proteggere e filtrare il sistema di posta da messaggi spam e dannosi.

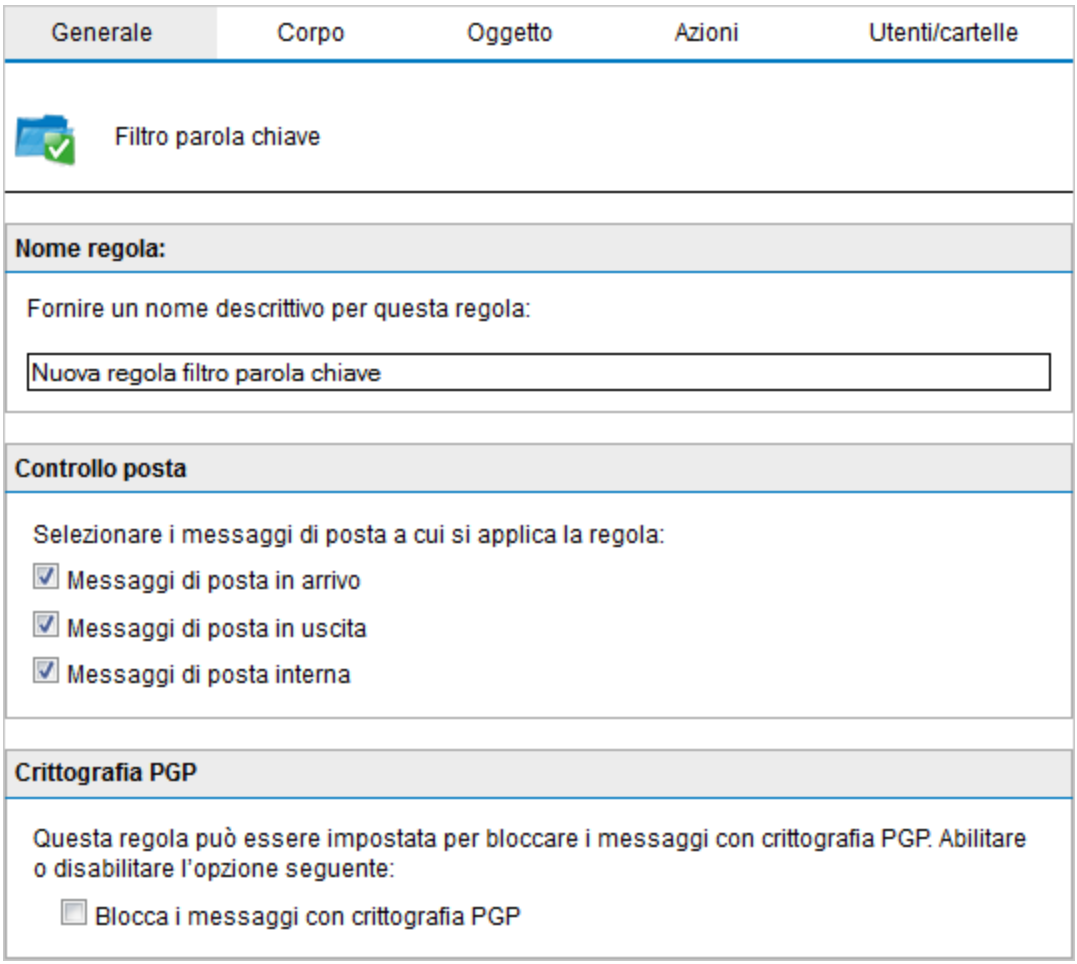
Accertarsi che GFI MailEssentials blocchi la posta indesiderata. A questo proposito, inviare messaggi di prova in entrata e in uscita composti appositamente per essere bloccati da GFI MailEssentials.

Passaggio 1: creazione di una regola di filtro dei contenuti

1. Avviare la console di GFI MailEssentials.

Selezionare **GFI MailEssentials > Filtro contenuti > nodo Filtro parola chiave**.

3. Fare clic su **Aggiungi regola...**.


Generale
Corpo
Oggetto
Azioni
Utenti/cartelle
Filtro parola chiave
Nome regola:
Fornire un nome descrittivo per questa regola:
Nuova regola filtro parola chiave
Controllo posta
Selezionare i messaggi di posta a cui si applica la regola:
Messaggi di posta in arrivo
Messaggi di posta in uscita
Messaggi di posta interna
Crittografia PGP
Questa regola può essere impostata per bloccare i messaggi con crittografia PGP. Abilitare o disabilitare l'opzione seguente:
Blocca i messaggi con crittografia PGP

Schermata 19: creazione di una regola di prova per il filtro parole chiave

4. In **Nome regola**, digitare `Regola di prova`.

5. Dalla scheda **Oggetto**, selezionare **Blocca messaggi se il contenuto corrisponde a queste condizioni (oggetto messaggio)**.

6. In **Modifica condizione**, digitare `Minaccia di prova` e fare clic su **Aggiungi condizione**.

7. Dalla scheda **Azioni**, abilitare **Blocca e-mail ed esegui l'azione seguente** quindi scegliere **E-mail in quarantena**.

8. Per salvare la regola, fare clic su **Applica**.

Passaggio 2: invio di un messaggio di prova in entrata

1. Da un account di posta esterno, creare un nuovo messaggio e digitare `Minaccia di prova` nell'oggetto.

2. Inviare il messaggio a uno degli account di posta interni.

Passaggio 3: invio di un messaggio di prova in uscita

1. Da un account di posta interno, creare un nuovo messaggio e digitare `Minaccia di prova` nell'oggetto.

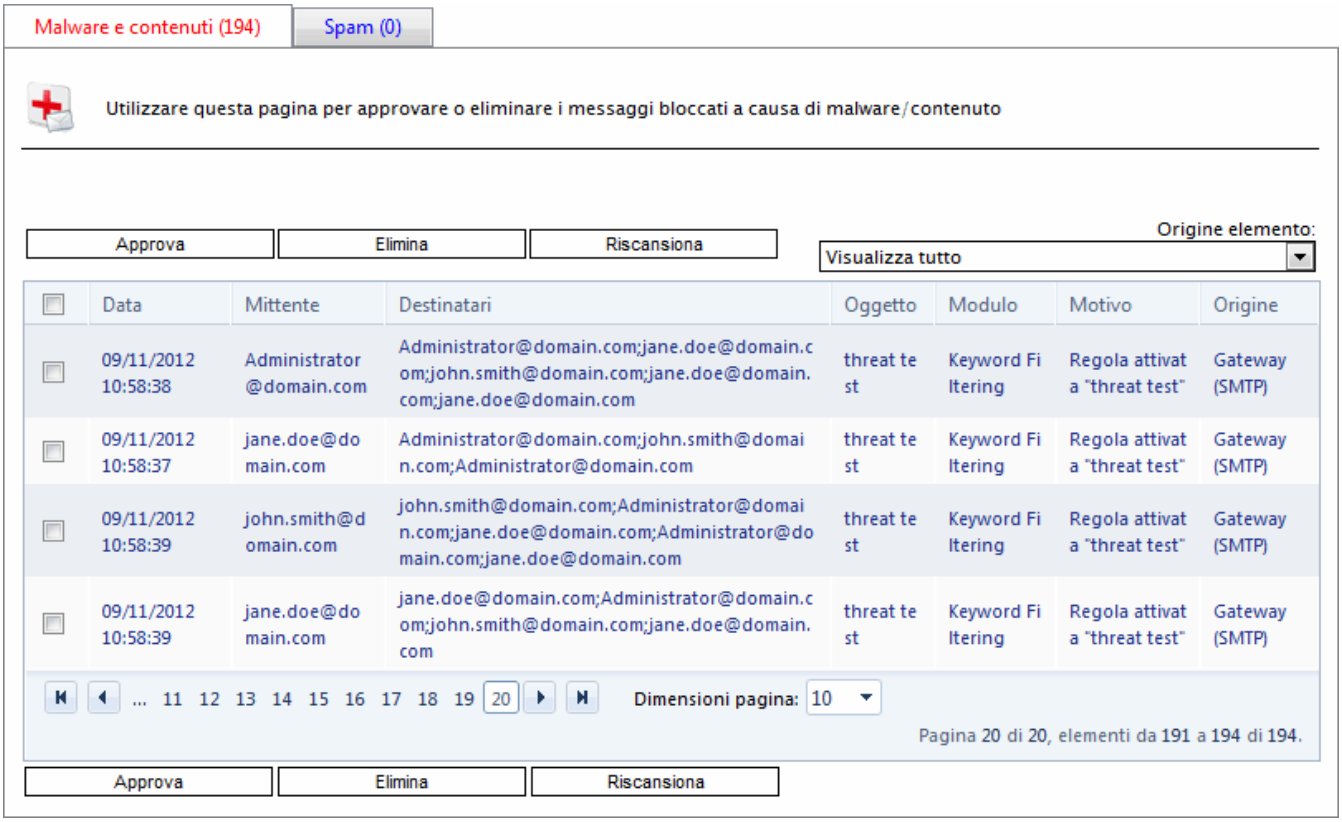
2. Inviare il messaggio a uno degli account di posta esterni.

Passaggio 4: conferma del blocco dei messaggi di prova

Verificare che i messaggi di prova sia in entrata che in uscita siano bloccati e inseriti nella quarantena. A tale scopo, procedere come segue:

1. Da GFI MailEssentials, accedere a **GFI MailEssentials Configuration > Quarantena > Oggi**

2. Assicurarsi che sia i messaggi di prova in uscita che in entrata siano elencati nella scheda **Malware e contenuti** con accanto la motivazione: **Regola attivata "Regola di prova"**.



Schermata 20: messaggio di prova bloccato da Regola di prova

NOTA

Al completamento della prova, eliminare o disabilitare la **Regola di prova** creata nel passaggio 1.

4 Stato di monitoraggio

GFI MailEssentials consente il monitoraggio dell'attività della posta elettronica in tempo reale oppure generando rapporti dell'attività della posta per un periodo di tempo specifico.

Modulo di monitoraggio	Descrizione
Dashboard	Il **Dashboard** di GFI MailEssentials fornisce informazioni in tempo reale che consentono di monitorare il prodotto. Per accedere alla Dashboard, selezionare **GFI MailEssentials > Dashboard**. Essa comprende: » Importanti informazioni statistiche relative ai messaggi bloccati. Per ulteriori informazioni, fare riferimento a Stato e statistiche (pagina 55). » Stato dei servizi di GFI MailEssentials. Per ulteriori informazioni, fare riferimento a Servizi (pagina 56). » Rappresentazione grafica dell'attività della posta. Per ulteriori informazioni, fare riferimento a Grafici (pagina 57). » Elenco dei messaggi elaborati. Per ulteriori informazioni, fare riferimento a Registri di elaborazione messaggi di posta elettronica (pagina 58). » Stato degli aggiornamenti software. Per ulteriori informazioni, fare riferimento a Aggiornamenti antivirus e antispam (pagina 60). » Record degli eventi importanti di GFI MailEssentials. Per ulteriori informazioni, fare riferimento a Registro eventi (pagina 61). » Registro delle attività di POP2Exchange. Per ulteriori informazioni, fare riferimento a Attività POP2Exchange (pagina 62).
Rapporti	GFI MailEssentials consente di creare rapporti sulla base dei dati registrati nel database. Per accedere a Creazione di rapporti, selezionare **GFI MailEssentials > Creazione di rapporti**. » **Abilitazione creazione di rapporti**: Per ulteriori informazioni, fare riferimento a Abilitazione/disabilitazione di creazione rapporti (pagina 62). » **Configura il database di creazione rapporti**: Per ulteriori informazioni, fare riferimento a Configurazione del database di creazione rapporti (pagina 69). » **Generazione rapporti:** Per ulteriori informazioni, fare riferimento a Generazione di un rapporto (pagina 63). » **Creazione di rapporti personalizzati**: Per ulteriori informazioni, fare riferimento a Rapporti personalizzati (pagina 66). » **Ricerca nel database di creazione rapporti**: Per ulteriori informazioni, fare riferimento a Ricerca nel database di creazione rapporti (pagina 67).

4.1 Dashboard

Il **Dashboard** di GFI MailEssentials fornisce informazioni in tempo reale che consentono di monitorare il prodotto. Per accedere alla Dashboard, selezionare **GFI MailEssentials > Dashboard**. Essa comprende:

» Importanti informazioni statistiche relative ai messaggi bloccati. Per ulteriori informazioni, fare riferimento a Stato e statistiche (pagina 55).

» Stato dei servizi di GFI MailEssentials. Per ulteriori informazioni, fare riferimento a Servizi (pagina 56).

» Rappresentazione grafica dell'attività della posta. Per ulteriori informazioni, fare riferimento a Grafici (pagina 57).

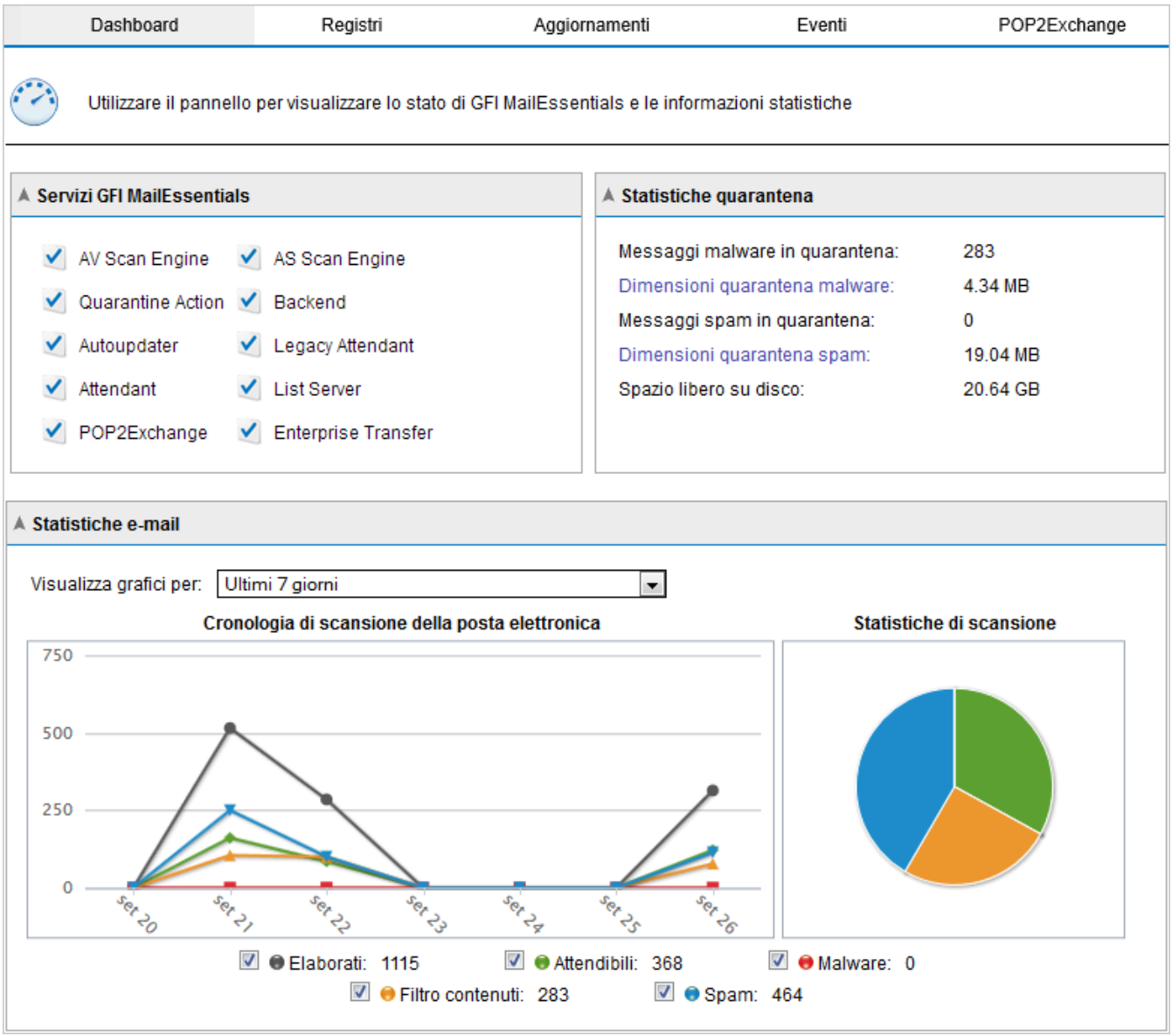
» Elenco dei messaggi elaborati. Per ulteriori informazioni, fare riferimento a Registri di elaborazione messaggi di posta elettronica (pagina 58).

» Stato degli aggiornamenti software. Per ulteriori informazioni, fare riferimento a Aggiornamenti antivirus e antispam (pagina 60).

» Record degli eventi importanti di GFI MailEssentials. Per ulteriori informazioni, fare riferimento a Registro eventi (pagina 61).

» Registro delle attività di POP2Exchange. Per ulteriori informazioni, fare riferimento a Attività POP2Exchange (pagina 62).

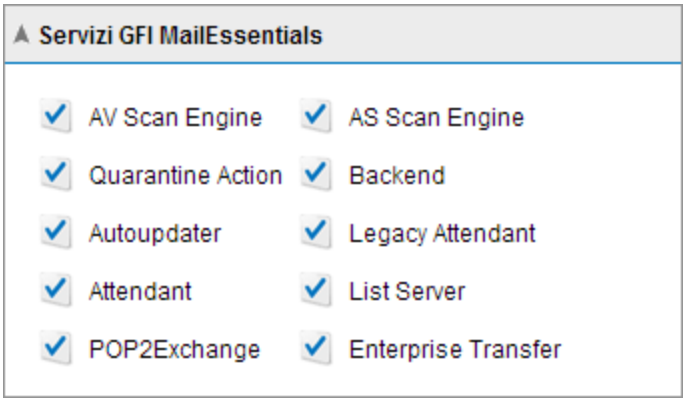
4.1.1 Stato e statistiche



Schermata 21: Dashboard GFI MailEssentials

Per aprire la Dashboard, selezionare **GFI MailEssentials > Dashboard**. Questa pagina mostra le statistiche, lo stato dei servizi e una rappresentazione grafica dell'attività della posta. Di seguito sono forniti maggiori dettagli su queste sezioni.

Servizi



Schermata 22: I servizi di GFI MailEssentials

L'area **Servizi** visualizza lo stato dei servizi di GFI MailEssentials.

» : indica che il servizio è avviato. Per arrestare il servizio, fare clic su questa icona.

» : indica che il servizio è arrestato. Per avviare un servizio arrestato, fare clic su questa icona.

I servizi possono essere avviati o arrestati anche dalla console Servizi Windows di Microsoft®. Per avviare la console dei servizi, accedere a **Start > Esegui**, digitare `services.msc`, quindi fare clic su **OK**.

Statistiche quarantena

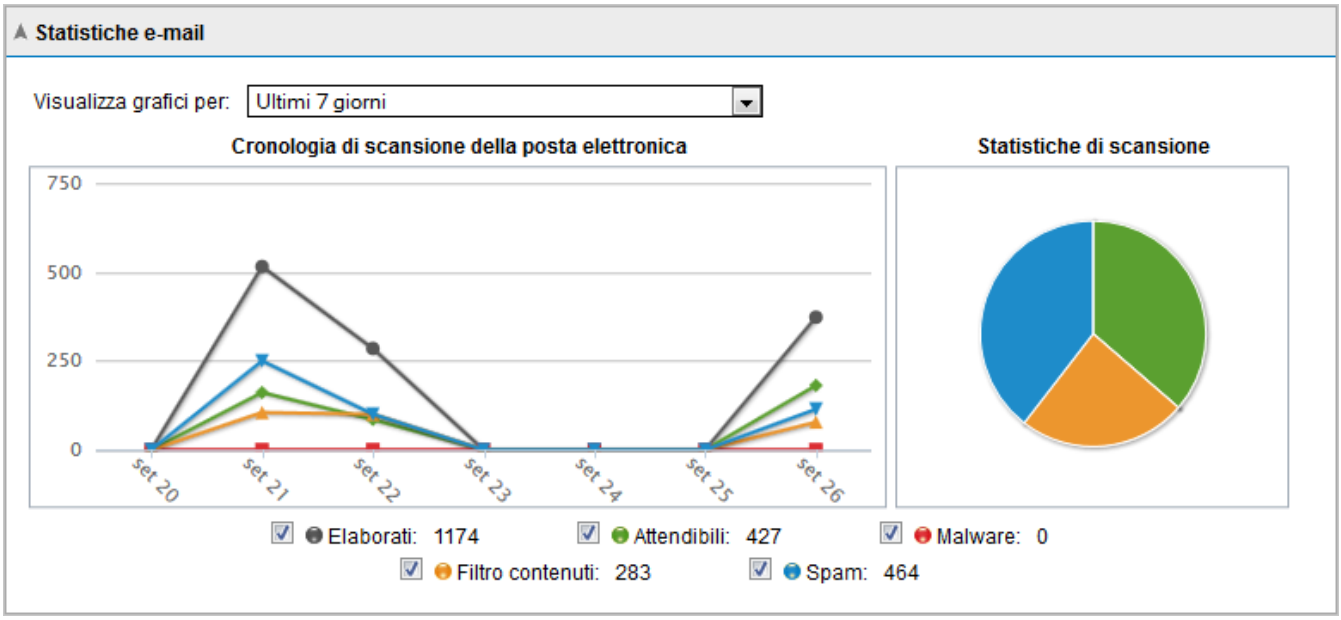
Statistiche quarantena
Messaggi malware in quarantena: 283
Dimensioni quarantena malware: 4.34 MB
Messaggi spam in quarantena: 0
Dimensioni quarantena spam: 19.04 MB
Spazio libero su disco: 20.64 GB

Schermata 23: Statistiche quarantena

L'area **Statistiche quarantena** mostra le seguenti informazioni statistiche:

Titolo statistica	Descrizione
Messaggi malware in quarantena	Numero di messaggi bloccati dai motori di Sicurezza e-mail e Filtro contenuti e poi archiviati nel Malware Quarantine Store.
Dimensioni quarantena malware	Dimensioni su disco del database di Malware Quarantine Store.
Messaggi spam in quarantena	Numero di messaggi bloccati dai motori antispam e archiviati in Spam Quarantine Store.
Dimensioni quarantena spam	Dimensioni su disco del database di Spam Quarantine Store.
Spazio libero su disco	Spazio libero su disco in cui vengono salvati i quarantine store.

Grafici

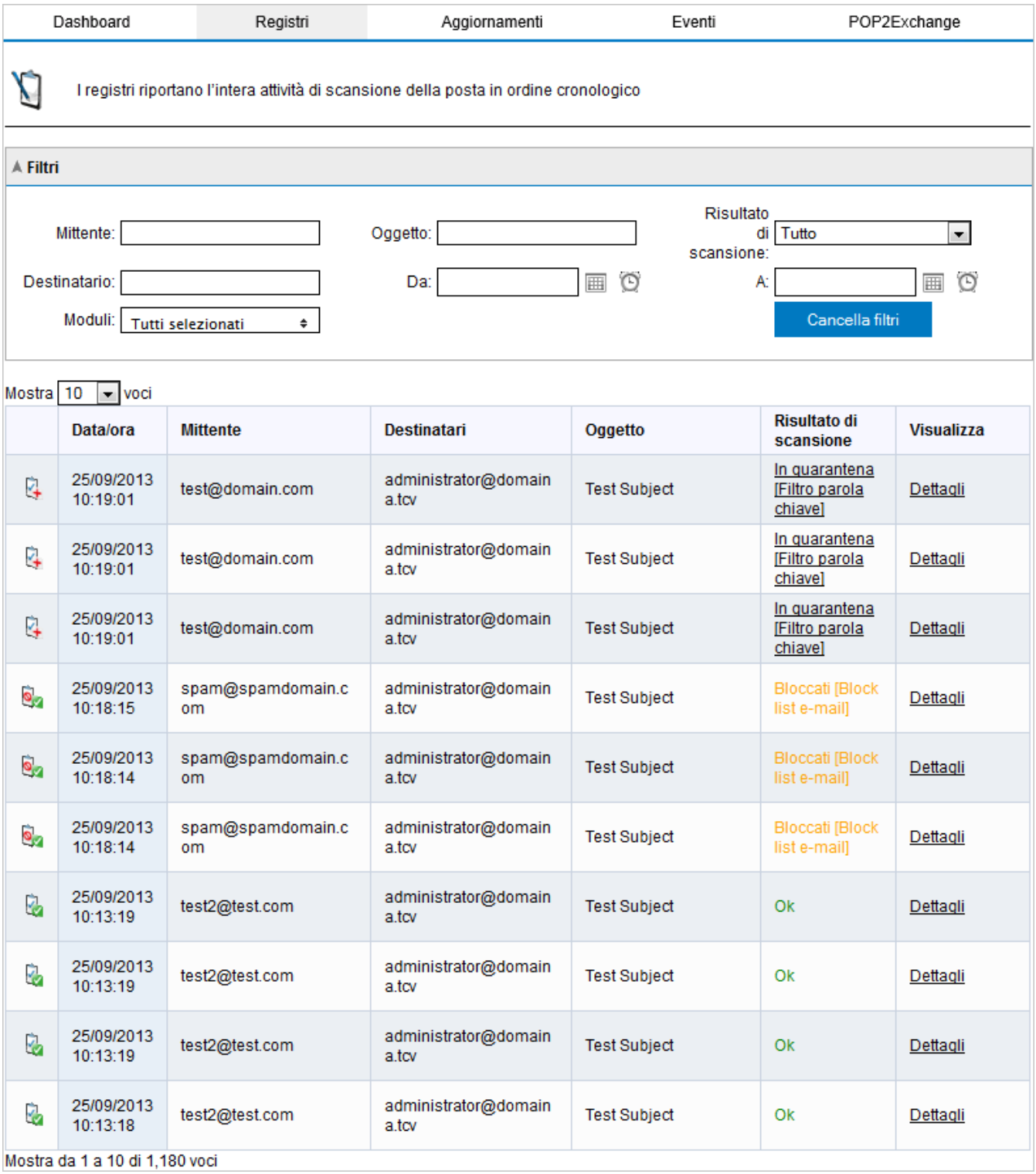


Schermata 24: Grafici del dashboard

L'area **Grafici** mostra informazioni grafiche sui messaggi elaborati da GFI MailEssentials. Dall'elenco a discesa, selezionare il periodo di tempo per mostrare le informazioni relative a quel periodo nei grafici.

Area	Descrizione
Visualizza grafici per	Consente di selezionare un periodo di visualizzazione dei grafici. Le opzioni disponibili sono: » Ultime 6 ore » Ultime 24 ore » Ultime 48 ore » Ultimi 7 giorni
Cronologia di scansione della posta elettronica (grafico dei tempi)	Mostra un grafico dei tempi in intervalli per il periodo di tempo selezionato. Il grafico illustra il numero di messaggi elaborati, attendibili, malware, di filtro contenuti e spam.
Statistiche di scansione (grafico a torta)	Una distribuzione grafica del numero totale di messaggi sicuri, inseriti in quarantena e non riusciti per il periodo di tempo selezionato.
Legenda	La legenda mostra il colore utilizzato nei grafici e il conteggio per ciascuna categoria.

4.1.2 Registri di elaborazione messaggi di posta elettronica


Dashboard
Registri
Aggiornamenti
Eventi
POP2Exchange
I registri riportano l'intera attività di scansione della posta in ordine cronologico
Filtri
Mittente:
Oggetto:
Risultato di scansione:
Tutto
Destinatario:
Da:
A:
Moduli:
Tutti selezionati
Cancella filtri
Mostra 10 voci
Data/ora
Mittente
Destinatari
Oggetto
Risultato di scansione
Visualizza
25/09/2013 10:19:01 test@domain.com administrator@domain a.tcv Test Subject In quarantena [Filtro parola chiave] Dettagli
25/09/2013 10:19:01 test@domain.com administrator@domain a.tcv Test Subject In quarantena [Filtro parola chiave] Dettagli
25/09/2013 10:19:01 test@domain.com administrator@domain a.tcv Test Subject In quarantena [Filtro parola chiave] Dettagli
25/09/2013 10:18:15 spam@spamdomain.com administrator@domain a.tcv Test Subject Bloccati [Block list e-mail] Dettagli
25/09/2013 10:18:14 spam@spamdomain.com administrator@domain a.tcv Test Subject Bloccati [Block list e-mail] Dettagli
25/09/2013 10:18:14 spam@spamdomain.com administrator@domain a.tcv Test Subject Bloccati [Block list e-mail] Dettagli
25/09/2013 10:13:19 test2@test.com administrator@domain a.tcv Test Subject Ok Dettagli
25/09/2013 10:13:19 test2@test.com administrator@domain a.tcv Test Subject Ok Dettagli
25/09/2013 10:13:19 test2@test.com administrator@domain a.tcv Test Subject Ok Dettagli
25/09/2013 10:13:18 test2@test.com administrator@domain a.tcv Test Subject Ok Dettagli
Mostra da 1 a 10 di 1,180 voci

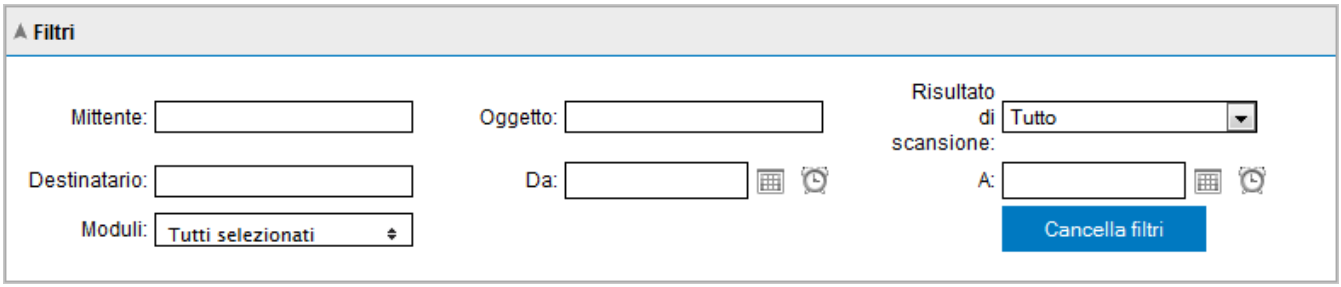
Schermata 25: Registri di elaborazione messaggi di posta elettronica

Da GFI MailEssentials Configuration, è possibile monitorare in tempo reale tutti i messaggi elaborati. Selezionare **GFI MailEssentials > Dashboard**, quindi fare clic sulla scheda **Registri** per visualizzare l'elenco dei messaggi elaborati. Per ciascun messaggio elaborato vengono visualizzati i seguenti dettagli:

- Data/ora
- Mittente
- Destinatari
- Oggetto
- Risultato di scansione: mostra l'azione effettuata sul messaggio.

Azione	Descrizione
OK	Il messaggio non viene bloccato da GFI MailEssentials e viene recapitato ai destinatari previsti.
In quarantena	Il messaggio bloccato da un motore o da un filtro che ha impostata l'azione di inserimento in quarantena. Per rivedere il messaggio, fare clic su **Quarantena**. **NOTA** Il messaggio non può essere visualizzato in anteprima in quarantena se è stato eliminato manualmente da essa.
Bloccato	Il messaggio è bloccato da un motore o da un filtro. L'azione intrapresa rispetta quella configurata per il motore specifico.
Eliminato	Il messaggio è stato bloccato da un motore o da un filtro con l'azione impostata di eliminazione dei messaggi rilevati.
Non riuscito	Il messaggio non può essere scansionato da GFI MailEssentials. Il messaggio viene spostato in una delle seguenti cartelle: *<GFI MailEssentials percorso di installazione>*\GFI\MailEssentials\EmailSecurity\failedmails\ *<GFI MailEssentials percorso di installazione>*\GFI\MailEssentials\AntiSpam\FailedMails\ Per ulteriori informazioni, fare riferimento a Messaggi di posta elettronica non riusciti (pagina 256).

Filtraggio dei registri di elaborazione dei messaggi



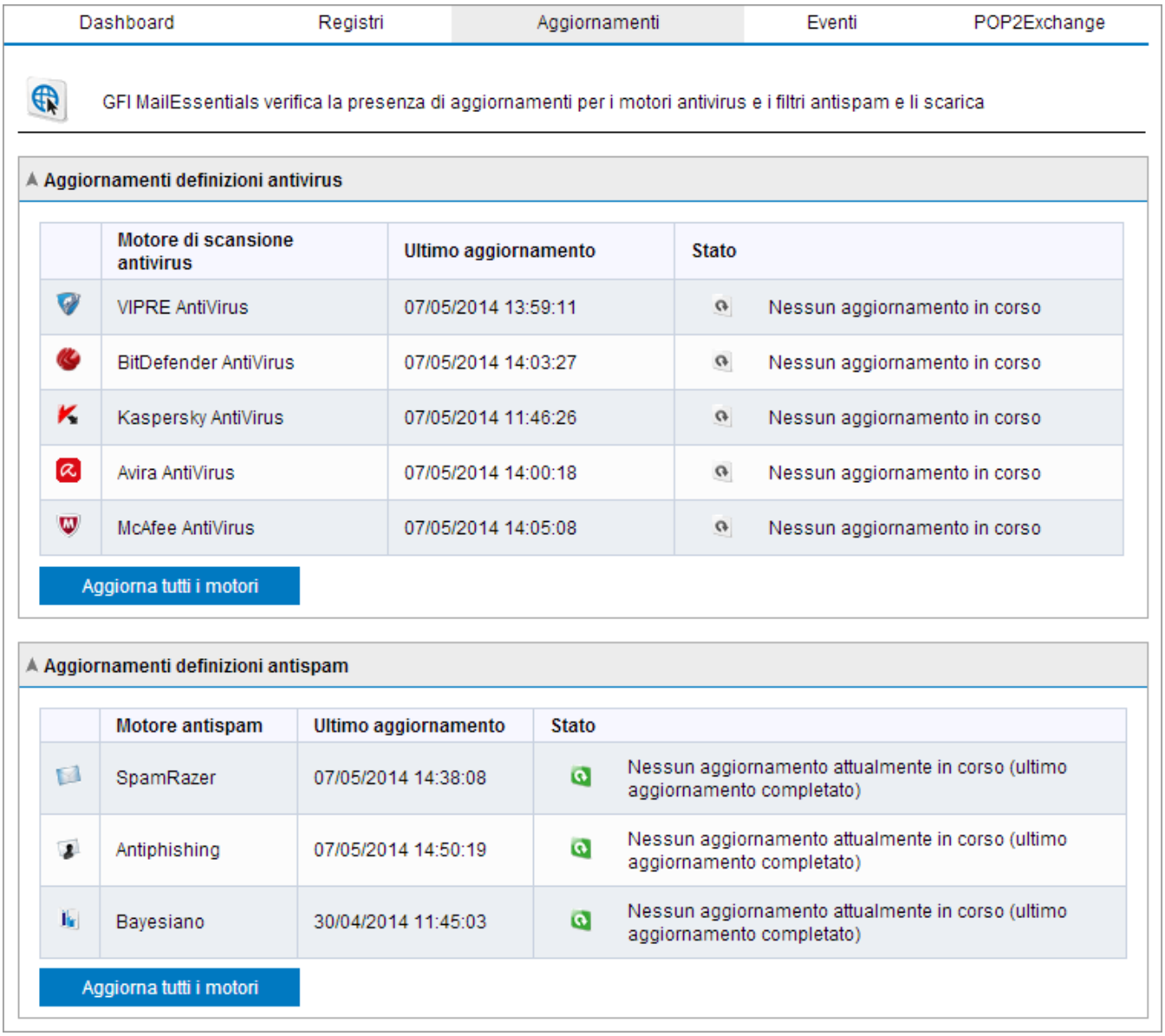
Schermata 26: filtro di elaborazione messaggi di posta elettronica

Il filtraggio dei registri di elaborazione dei messaggi di posta semplifica la procedura di revisione fornendo la possibilità di individuare messaggi specifici. Dall'area **Filtro**, indicare uno dei seguenti criteri:

Filtro	Descrizione
Mittente	Specificare l'indirizzo di posta completo o parziale per visualizzare solo i messaggi inviati da mittenti corrispondenti.
Destinatario	Specificare l'indirizzo di posta completo o parziale per visualizzare solo i messaggi inviati a destinatari corrispondenti.
Oggetto	Specificare l'oggetto del messaggio di posta completo o parziale per visualizzare solo i messaggi con un oggetto corrispondente.
Risultato di scansione	Dall'elenco a discesa, scegliere se visualizzare solo i messaggi con un risultato di scansione particolare (ad esempio, solo i messaggi inseriti in quarantena).
Da e a	Indicare una data e un intervallo di date per visualizzare i messaggi elaborati in quel periodo specifico.

NOTA
Per rimuovere i filtri indicati e mostrare tutti i registri di posta, fare clic su **Cancella filtri**.

4.1.3 Aggiornamenti antivirus e antispam



Schermata 27: aggiornamenti motori di scansione antivirus

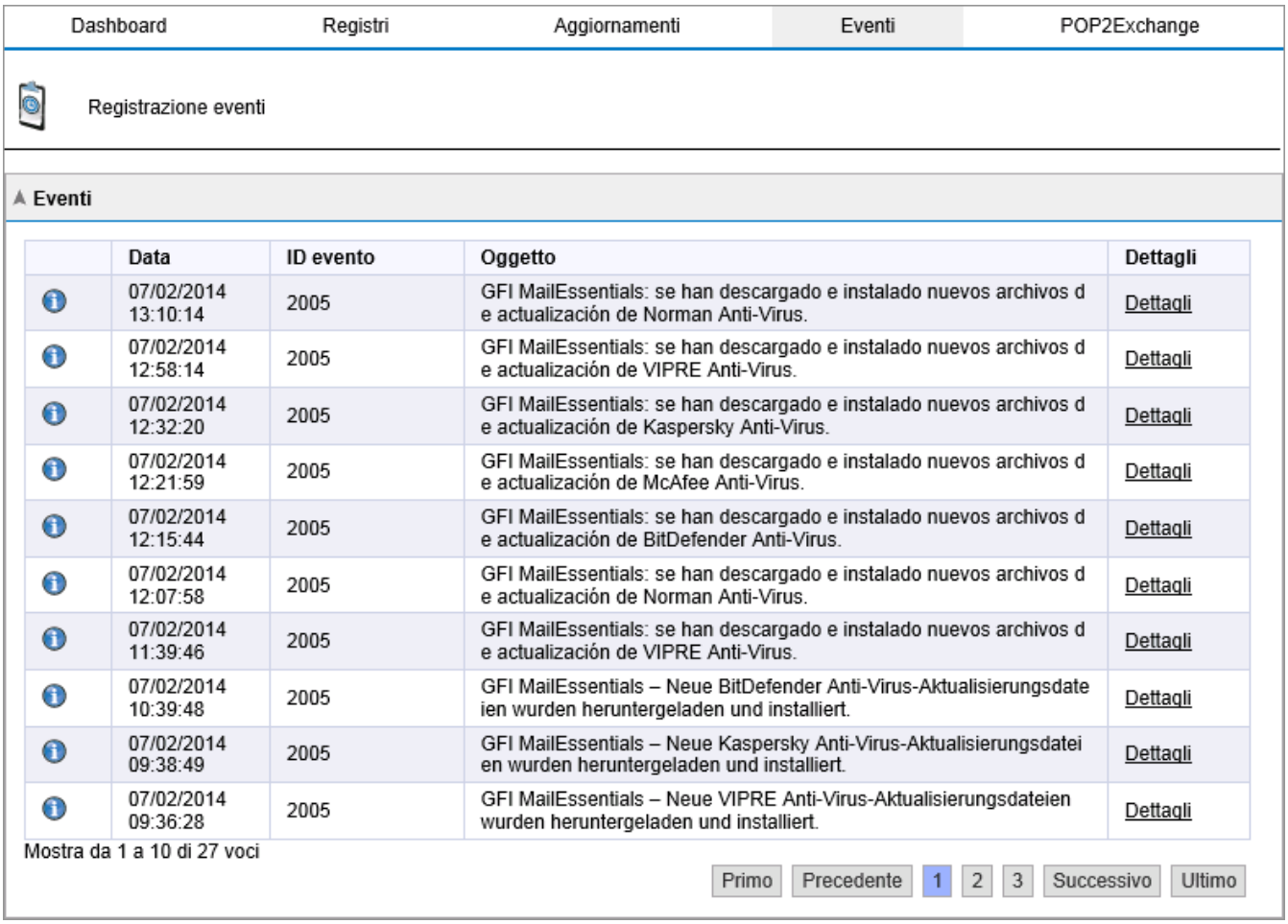
Gli aggiornamenti dei motori di scansione antivirus e antispam possono essere monitorati da una pagina centrale. Selezionare **GFI MailEssentials > Dashboard**, quindi fare clic sulla scheda **Aggiornamenti** per rivedere lo stato e le date in cui sono stati aggiornati per l'ultima volta i motori di scansione.

Per controllare la presenza di aggiornamenti e scaricarli, far clic su **Aggiorna tutti i motori**.

Viene verificata la presenza di aggiornamenti, per poi scaricarli in base a quanto configurato nelle pagine di configurazione dei motori. Andare alla pagina di configurazione di ciascun motore e selezionare la scheda **Aggiornamenti** per configurarne le impostazioni di aggiornamento.

NOTA
Gli aggiornamenti di ciascun motore vengono verificati e scaricati in sequenza (un aggiornamento di motore per volta).

4.1.4 Registro eventi



Schermata 28: Registro eventi

Dalla configurazione di GFI MailEssentials è possibile monitorare gli eventi importanti correlati alla funzionalità di GFI MailEssentials. Esempi di istanze che attivano gli eventi:

- completamento di aggiornamenti motore antispam
- il database di creazione rapporti raggiunge 1,7 GB e GFI MailEssentials passa a un nuovo database
- meno di 1 GB di spazio libero su disco nella partizione dove è salvata la quarantena

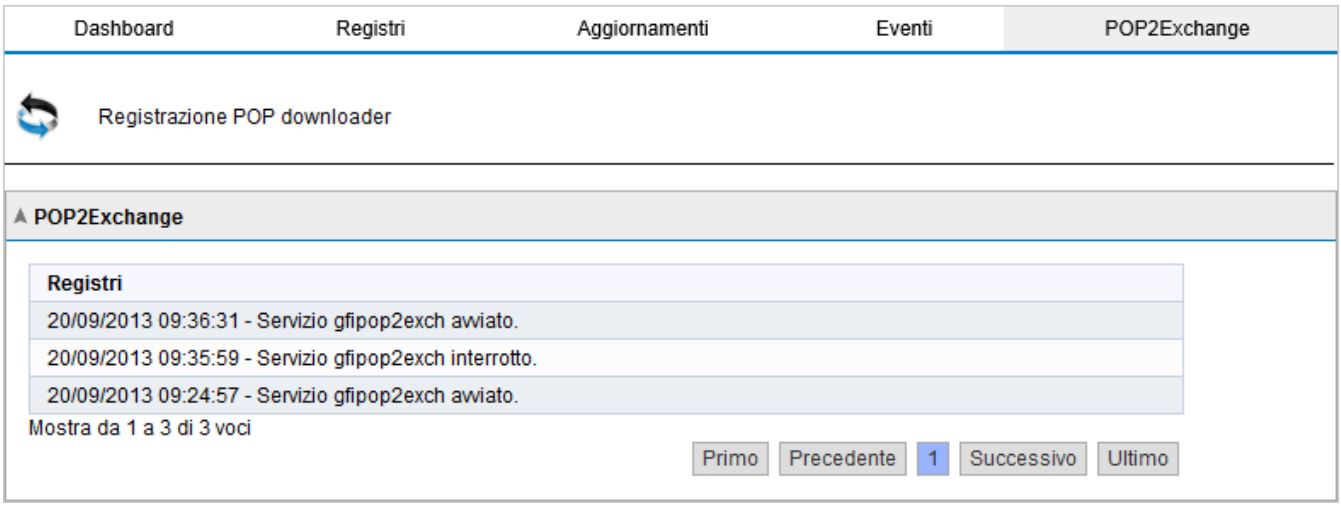
Selezionare **GFI MailEssentials > Dashboard**, quindi fare clic sulla scheda **Eventi** per visualizzare l'elenco degli eventi. Sono visualizzate le seguenti informazioni per ciascun evento:

- Data/ora
- ID evento: a ciascun tipo di evento di GFI MailEssentials viene assegnato un identificatore.
- Oggetto

Per visualizzare ulteriori informazioni su un evento specifico, fare clic su **Dettagli**.

Gli eventi GFI MailEssentials sono disponibili anche dal Visualizzatore eventi di Windows al percorso **Registri applicazioni e servizi** > GFI MailEssentials.

4.1.5 Attività POP2Exchange



Schermata 29: registro POP2Exchange

Da GFI MailEssentials è possibile monitorare l'attività di POP2Exchange in tempo reale. Selezionare **GFI MailEssentials** > **Dashboard**, quindi fare clic sulla scheda **POP2Exchange**.

> **NOTA**
> Per ulteriori informazioni, fare riferimento a POP2Exchange - Download messaggi dal server POP3 (pagina 259).

4.2 Rapporti

GFI MailEssentials consente di creare rapporti sulla base dei dati registrati nel database.

Per accedere a Creazione di rapporti, selezionare **GFI MailEssentials** > **Creazione di rapporti**.

» **Abilitazione creazione di rapporti**: Per ulteriori informazioni, fare riferimento a Abilitazione/disabilitazione di creazione rapporti (pagina 62).

» **Configura il database di creazione rapporti**: Per ulteriori informazioni, fare riferimento a Configurazione del database di creazione rapporti (pagina 69).

» **Generazione rapporti:** Per ulteriori informazioni, fare riferimento a Generazione di un rapporto (pagina 63).

» **Creazione di rapporti personalizzati**: Per ulteriori informazioni, fare riferimento a Rapporti personalizzati (pagina 66).

» **Ricerca nel database di creazione rapporti**: Per ulteriori informazioni, fare riferimento a Ricerca nel database di creazione rapporti (pagina 67).

4.2.1 Abilitazione/disabilitazione di creazione rapporti

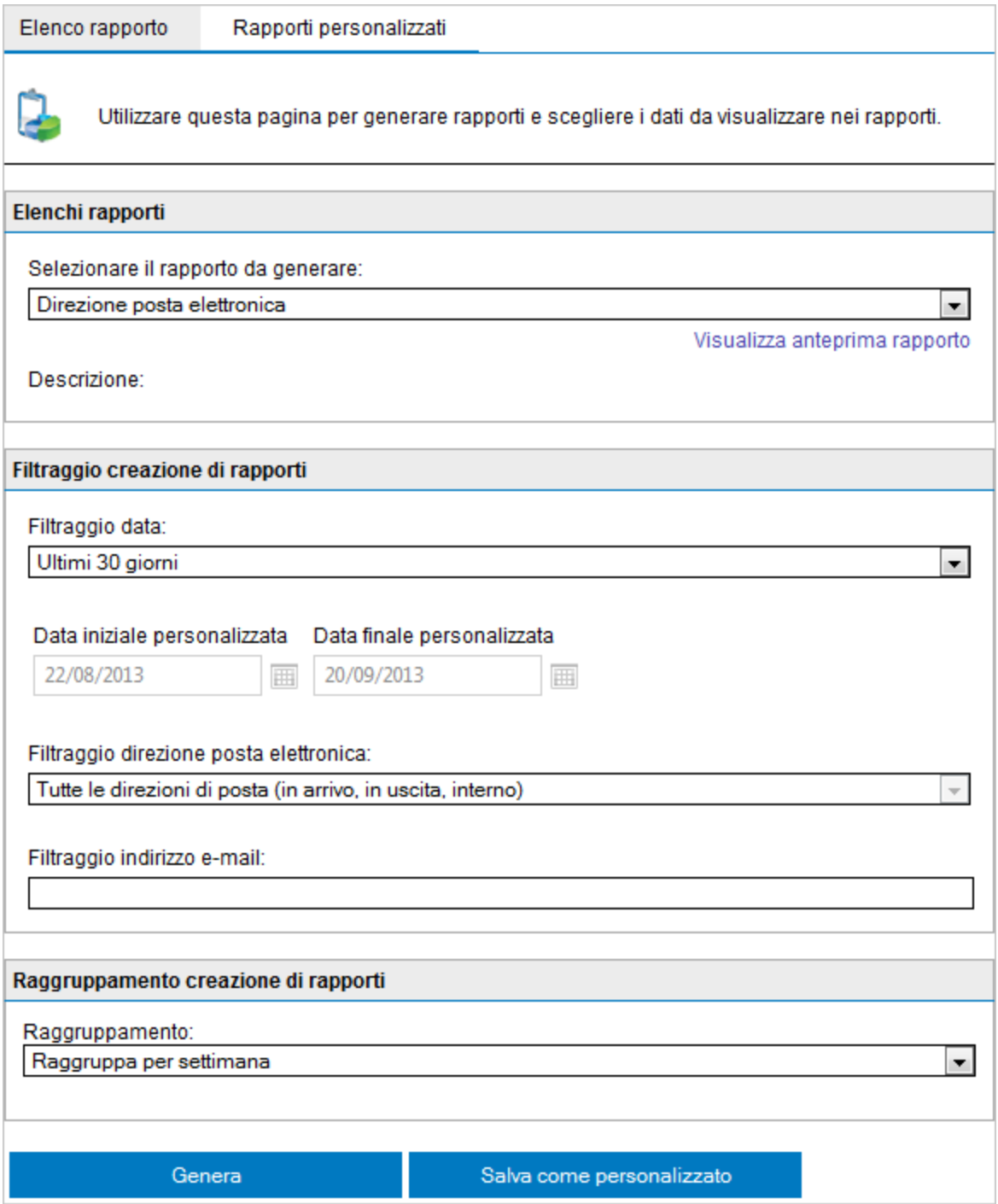
Per impostazione predefinita, Creazione rapporti è abilitata e l'attività della posta viene registrata in un database Firebird situato nella cartella:

<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\data\

Selezionare **Creazione report > nodo Impostazioni** e selezionare o deselezionare **Abilita creazione di rapporti**, rispettivamente per abilitare o disabilitare la funzione.

4.2.2 Generazione di un rapporto

1. Da GFI MailEssentials configuration, selezionare **GFI MailEssentials > Creazione report > Rapporti**.



Schermata 30: creazione di un rapporto

2. Dalla scheda **Elenco rapporto**, configurare le seguenti opzioni di rapporti:

Opzione	Descrizione
Tipo di rapporto	Selezione del tipo di rapporto da generare: » **Messaggi di posta elettronica bloccati**: mostra i messaggi totali bloccati dai filtri antispam e antimalware per ciascuna direzione della posta (in entrata, in uscita e interna) sul totale di tutti i messaggi elaborati. » **Grafico messaggi di posta elettronica bloccati**: mostra graficamente i messaggi totali bloccati dai filtri antispam e antimalware per ciascuna direzione della posta (in entrata, in uscita e interna) sul totale di tutti i messaggi elaborati. » **Grafico direzione posta elettronica**: mostra graficamente i messaggi totali elaborati per ciascuna direzione della posta (in entrata, in uscita e interna). » **Direzione posta**: mostra i messaggi totali elaborati per ciascuna direzione della posta (in entrata, in uscita e interna). » **Rapporto utente**: mostra il numero di messaggi di posta bloccati e consentiti per ciascun indirizzo di posta. » **Filtro antispam**: visualizza il numero totale di messaggi bloccati da ciascun filtro spam. » **Grafico filtro antispam**: visualizza il numero totale di messaggi bloccati da ciascun filtro antispam. Per visualizzare in anteprima il rapporto, fare clic su **Visualizza anteprima rapporto**.
Filtraggio data	Selezionare l'intervallo di date del rapporto. Al momento di selezionare **Intervallo di date personalizzato**, indicare il periodo per cui visualizzare i dati dai controlli del calendario **Data iniziale personalizzata** e **Data finale personalizzata**.
Filtraggio direzioni posta elettronica	Selezionare una direzione specifica per la posta per la visualizzazione dei dati oppure fare clic su **Tutte le direzioni di posta (in entrata, esterna, interna)** per visualizzare dati provenienti da tutte le direzioni.
Filtraggio indirizzo e-mail	Digitare un indirizzo e-mail per visualizzare le informazioni di rapporto specifiche di quell'indirizzo di posta.
Raggruppamento creazione di rapporti	Indicare il modo in cui raggruppare i dati. Le opzioni disponibili sono: » **Raggruppa per giorno** » **Raggruppa per settimana** » **Raggruppa per mese** » **Raggruppa per anno**

3. Per creare e visualizzare il rapporto, fare clic su **Genera** oppure fare clic su **Salva come personalizzato** per salvare le impostazioni del rapporto per riutilizzarlo in un secondo momento.

Schermata 31: rapporto grafico messaggi di posta elettronica bloccati

Funzioni rapporto

Utilizzare la barra degli strumenti superiore del rapporto per svolgere le seguenti funzioni:

Funzioni	Icona	Descrizione
Stampa		Selezionare per stampare il rapporto.
Stampa la pagina attuale		Stampa il documento visualizzato.
Navigazione		Utilizzare questa barra degli strumenti per navigare tra le pagine del rapporto.
Salva		Selezionare il formato in cui salvare il rapporto, quindi fare clic su **Salva**. Indicare il percorso in cui salvare il rapporto.

4.2.3 Rapporti personalizzati

I rapporti personalizzati consentono di salvare specifici parametri dei rapporti (ad esempio, un tipo di record per un periodo specifico di ora/data) e generarli in base a una pianificazione. Per automatizzare la generazione dei rapporti, utilizzare questa funzione.

Configurazione rapporti personalizzati

1. Da GFI MailEssentials configuration, selezionare **GFI MailEssentials > Creazione di rapporti > Rapporti**.

2. Selezionare la scheda **Rapporti personalizzati**, quindi fare clic su **Nuovo**.

3. Configurare le opzioni seguenti:

Opzione	Descrizione
Tipo di rapporto	Selezione del tipo di rapporto da generare: » **Messaggi di posta elettronica bloccati**: mostra i messaggi totali bloccati dai filtri antispam e antimalware per ciascuna direzione della posta (in entrata, in uscita e interna) sul totale di tutti i messaggi elaborati. » **Grafico messaggi di posta elettronica bloccati**: mostra graficamente i messaggi totali bloccati dai filtri antispam e antimalware per ciascuna direzione della posta (in entrata, in uscita e interna) sul totale di tutti i messaggi elaborati. » **Grafico direzione posta elettronica**: mostra graficamente i messaggi totali elaborati per ciascuna direzione della posta (in entrata, in uscita e interna). » **Direzione posta**: mostra i messaggi totali elaborati per ciascuna direzione della posta (in entrata, in uscita e interna). » **Rapporto utente**: mostra il numero di messaggi di posta bloccati e consentiti per ciascun indirizzo di posta. » **Filtro antispam**: visualizza il numero totale di messaggi bloccati da ciascun filtro spam. » **Grafico filtro antispam**: visualizza il numero totale di messaggi bloccati da ciascun filtro antispam. Per visualizzare in anteprima il rapporto, fare clic su **Visualizza anteprima rapporto**.
Filtraggio data	Selezionare l'intervallo di date del rapporto. Al momento di selezionare **Intervallo di date personalizzato**, indicare il periodo per cui visualizzare i dati dai controlli del calendario **Data iniziale personalizzata** e **Data finale personalizzata**.
Filtraggio direzioni posta elettronica	Selezionare una direzione specifica per la posta per la visualizzazione dei dati oppure fare clic su **Tutte le direzioni di posta (in entrata, esterna, interna)** per visualizzare dati provenienti da tutte le direzioni.
Filtraggio indirizzo e-mail	Digitare un indirizzo e-mail per visualizzare le informazioni di rapporto specifiche di quell'indirizzo di posta.
Raggruppamento creazione di rapporti	Indicare il modo in cui raggruppare i dati. Le opzioni disponibili sono: » **Raggruppa per giorno** » **Raggruppa per settimana** » **Raggruppa per mese** » **Raggruppa per anno**

4. In alternativa, abilitare la casella di controllo **Invia ogni** e configurare una combinazione data/ora affinché il rapporto sia generato a una data/ora specifica. Fare clic su **Aggiungi regola** per salvare l'ora di generazione del rapporto.

NOTA
per eliminare una regola, selezionare un orario di generazione del rapporto esistente, quindi fare clic su **Elimina**.

5. Scegliere se inviare il rapporto per posta o salvarlo su disco. Per inviare il rapporto per posta, selezionare **Invia per e-mail** e fornire l'indirizzo di posta a cui è stato inviato il messaggio. Per salvare il rapporto su disco, selezionare **Salva su disco**, quindi fornire un percorso di salvataggio del file e il relativo formato.

6. Per salvare il rapporto appena creato, fare clic su **Salva**.

4.2.4 Generazione di rapporti personalizzati

Per generare un rapporto personalizzato:

1. Da GFI MailEssentials configuration, selezionare **GFI MailEssentials > Creazione di rapporti > Rapporti**.

2. Dalla scheda **Rapporti personalizzati**, selezionare un rapporto da generare.

3. Fare clic su **Genera**.

4.2.5 Eliminazione rapporti personalizzati

Per eliminare un rapporto personalizzato:

1. Da GFI MailEssentials configuration, selezionare **GFI MailEssentials > Creazione di rapporti > Rapporti**.

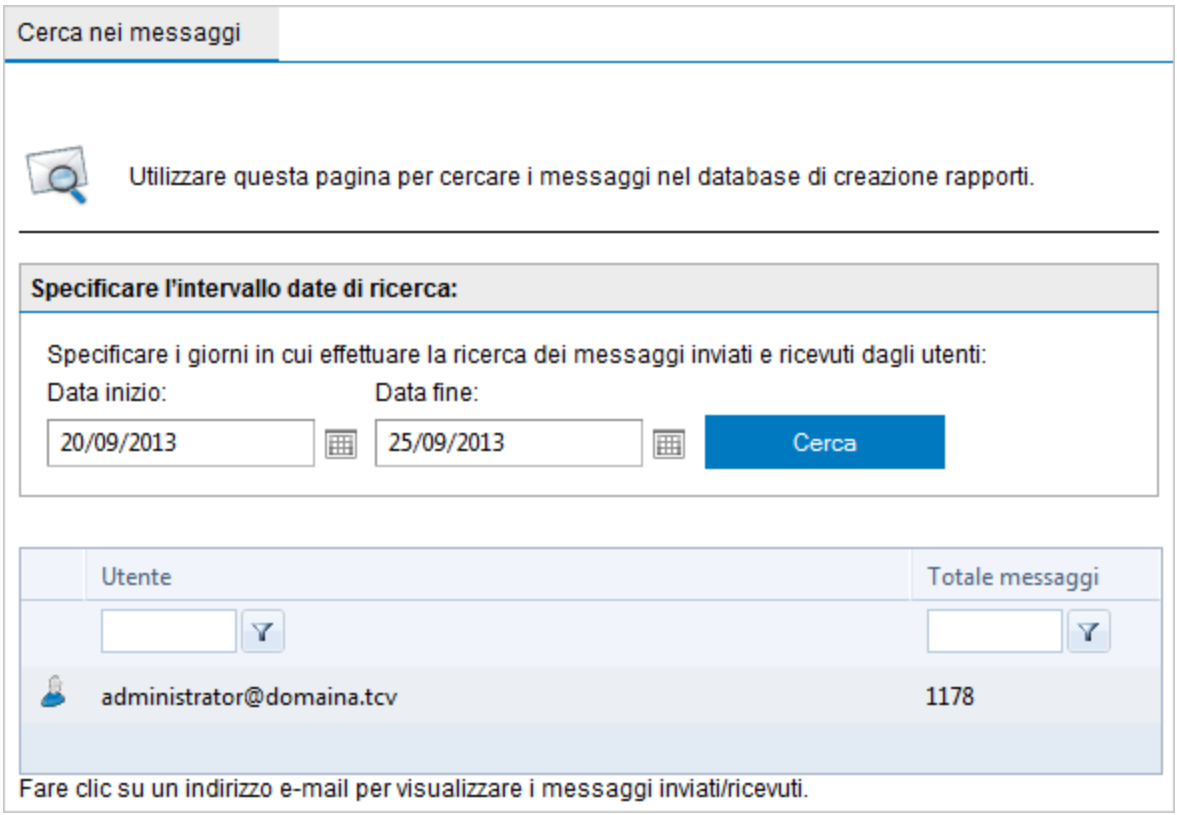
2. Dalla scheda **Rapporti personalizzati**, selezionare un rapporto da eliminare.

3. Fare clic su **Elimina**.

4.2.6 Ricerca nel database di creazione rapporti

GFI MailEssentials archivia alcune proprietà di tutti i messaggi elaborati nel database di creazione rapporti. GFI MailEssentials consente di effettuare ricerche nel database di creazione rapporti per l'individuazione dei messaggi elaborati. Per cercare nel database di creazione rapporti:

1. Da GFI MailEssentials Configuration, selezionare **GFI MailEssentials > Creazione di report > Cerca**.

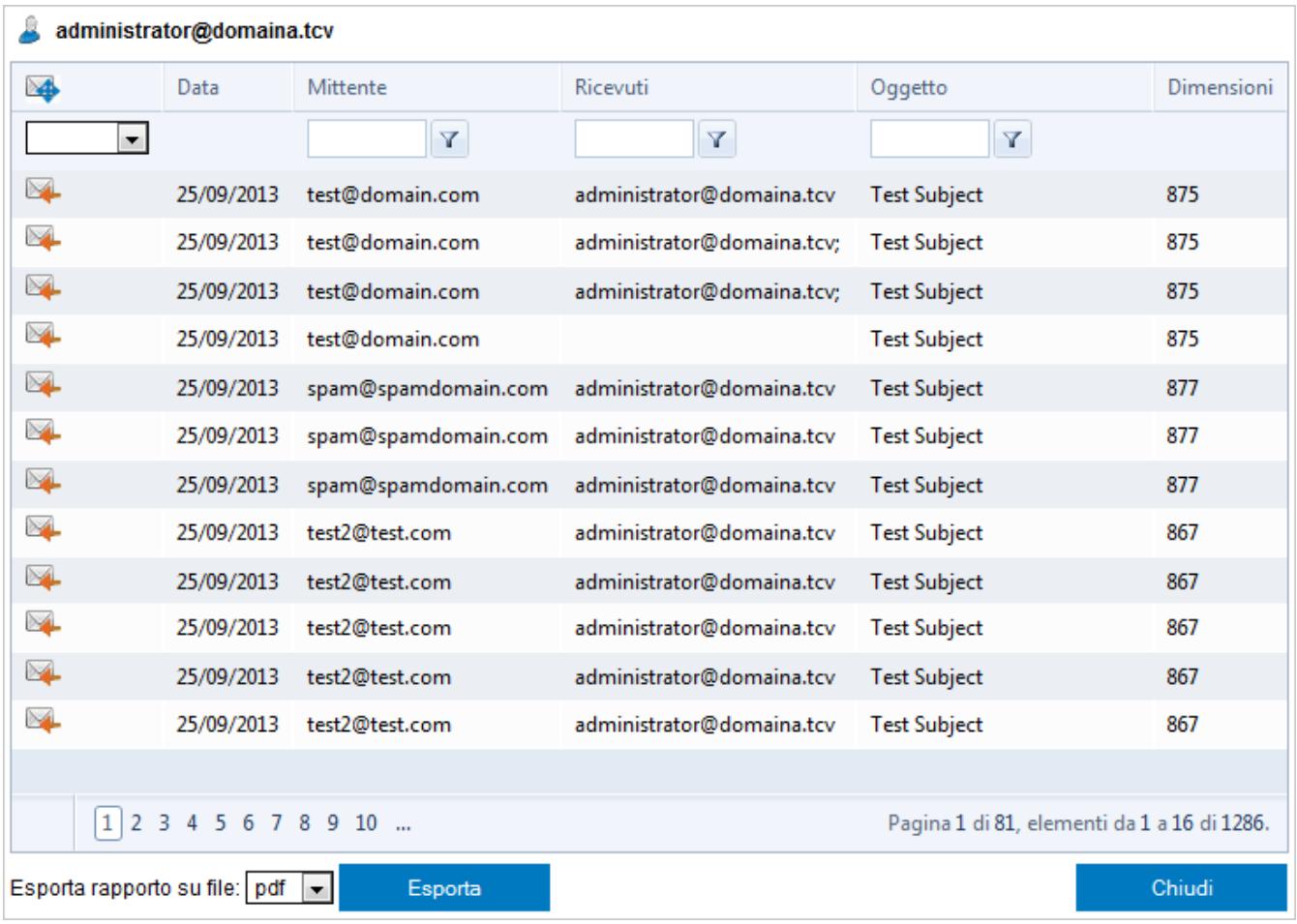

Cerca nei messaggi
Utilizzare questa pagina per cercare i messaggi nel database di creazione rapporti.
Specificare l'intervallo date di ricerca:
Specificare i giorni in cui effettuare la ricerca dei messaggi inviati e ricevuti dagli utenti:
Data inizio:
Data fine:
20/09/2013
25/09/2013
Cerca
Utente
Totale messaggi
administrator@domaina.tcv
1178
Fare clic su un indirizzo e-mail per visualizzare i messaggi inviati/ricevuti.

Schermata 32: Ricerca nel database di creazione rapporti

2. Indicare i criteri di ricerca

Criteri di ricerca	Descrizione
Data inizio e **data fine**	Selezionare l'intervallo di date per filtrare i messaggi di quel periodo. Fare clic su **Cerca**.
Utente	Filtrare i risultati dell'indirizzo di posta elettronica. Digitare un numero e fare clic su per indicare le condizioni.
Totale messaggi	Filtra gli utenti in base alla quantità di messaggi elaborati. Digitare un numero e fare clic su per indicare le condizioni.

3. Viene visualizzato l'elenco degli utenti corrispondenti. Fare clic su un indirizzo e-mail per visualizzare un rapporto dettagliato dei messaggi elaborati per quell'indirizzo di posta.


administrator@domaina.tcv
Data
Mittente
Ricevuti
Oggetto
Dimensioni
25/09/2013 test@domain.com administrator@domaina.tcv Test Subject 875
25/09/2013 test@domain.com administrator@domaina.tcv; Test Subject 875
25/09/2013 test@domain.com administrator@domaina.tcv; Test Subject 875
25/09/2013 test@domain.com Test Subject 875
25/09/2013 spam@spamdomain.com administrator@domaina.tcv Test Subject 877
25/09/2013 spam@spamdomain.com administrator@domaina.tcv Test Subject 877
25/09/2013 spam@spamdomain.com administrator@domaina.tcv Test Subject 877
25/09/2013 test2@test.com administrator@domaina.tcv Test Subject 867
25/09/2013 test2@test.com administrator@domaina.tcv Test Subject 867
25/09/2013 test2@test.com administrator@domaina.tcv Test Subject 867
25/09/2013 test2@test.com administrator@domaina.tcv Test Subject 867
25/09/2013 test2@test.com administrator@domaina.tcv Test Subject 867
1 2 3 4 5 6 7 8 9 10 ...
Pagina 1 di 81, elementi da 1 a 16 di 1286.
Esporta rapporto su file: pdf
Esporta
Chiudi

Schermata 33: risultati di ricerca database Rapporti

4. (Facoltativo) Dal rapporto, filtrare i dati in base alla direzione della posta, al mittente, al ricevente o all'oggetto.

5. Per esportare il rapporto in un altro formato, selezionarlo e quindi fare clic su **Esporta**.

4.2.7 Configurazione del database di creazione rapporti

Per impostazione predefinita, GFI MailEssentials utilizza un database Firebird **reports.fdb** situato in:

<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\data\

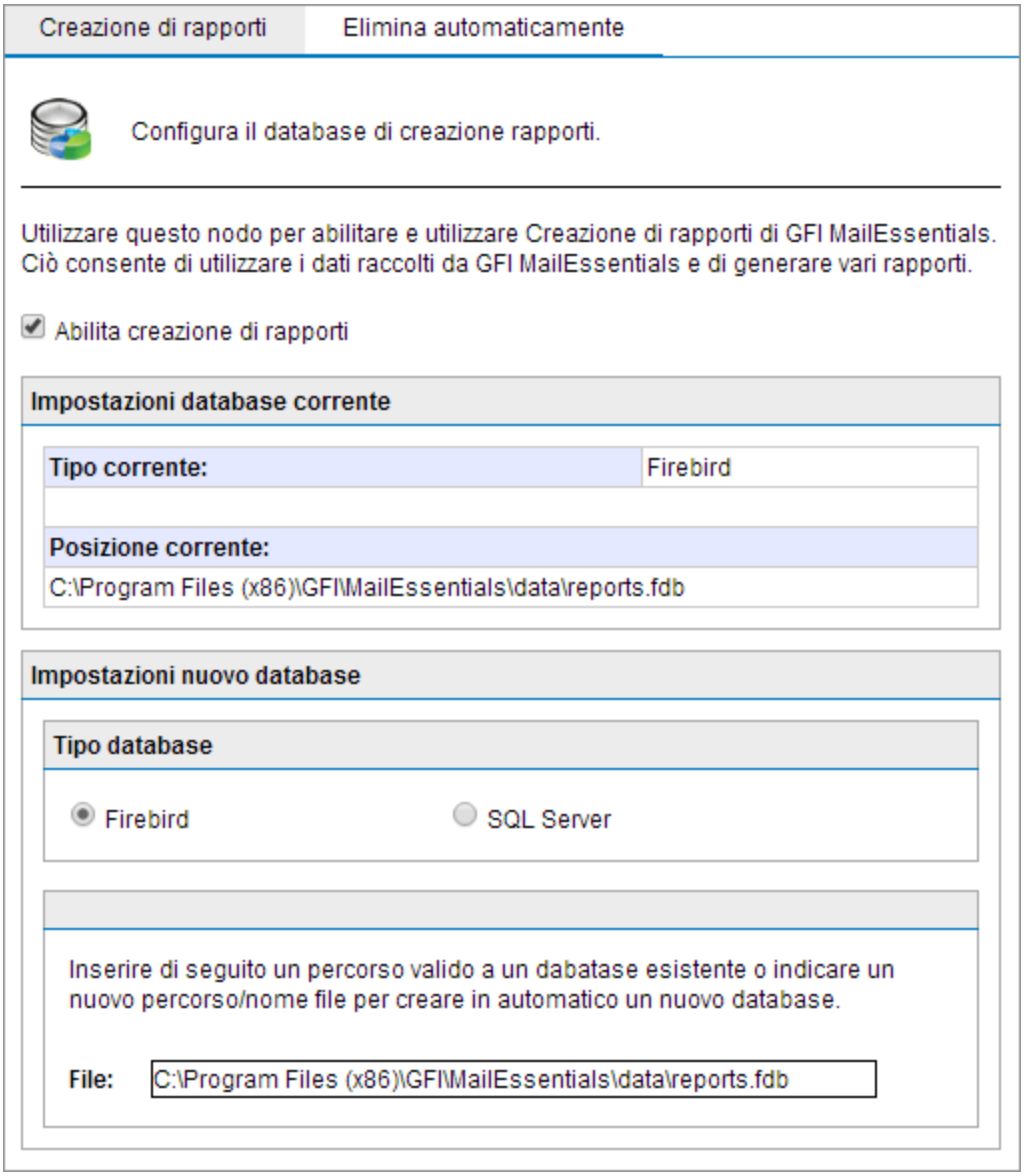
È anche possibile utilizzare un database Microsoft® SQL Server per i rapporti.

» Configurazione di un database back-end Firebird

» Configurazione di un database back-end Microsoft® SQL Server

» Configurazione dell'eliminazione automatica del database

Configurazione di un database back-end Firebird


Creazione di rapporti
Elimina automaticamente
Configura il database di creazione rapporti.
Utilizzare questo nodo per abilitare e utilizzare Creazione di rapporti di GFI MailEssentials.
Ciò consente di utilizzare i dati raccolti da GFI MailEssentials e di generare vari rapporti.
Abilita creazione di rapporti
Impostazioni database corrente
Tipo corrente:
Firebird
Posizione corrente:
C:\Program Files (x86)\GFI\MailEssentials\data\reports.fdb
Impostazioni nuovo database
Tipo database
Firebird
SQL Server
Inserire di seguito un percorso valido a un dabatase esistente o indicare un nuovo percorso/nome file per creare in automatico un nuovo database.
File:
C:\Program Files (x86)\GFI\MailEssentials\data\reports.fdb

Schermata 34: Configurazione di un database back-end Firebird

1. Selezionare **Creazione di rapporti > Impostazioni**.

2. Selezionare **Firebird**.

3. Immettere il percorso completo, incluso il nome del file (e l'estensione .fdb) del file di database. Se si indica solo il nome file, il file di database viene creato nel seguente percorso predefinito:

`<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\data\`

4. Fare clic su **Applica**.

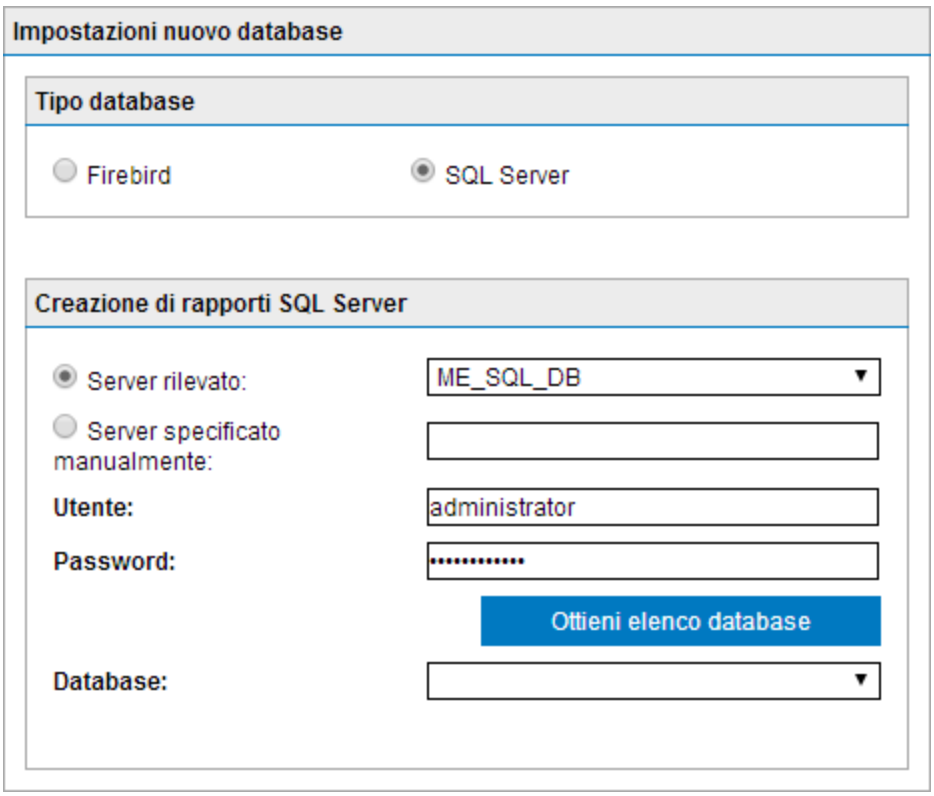
NOTA
Quando il database raggiunge le dimensioni di 7 GB, viene inviata una notifica e-mail all'amministratore perché potrebbe compromettere le prestazioni. In questo caso, si consiglia di utilizzare la funzione di eliminazione automatica per la rimozione delle e-mail antecedenti a una data specifica.

Configurazione di un database back-end Microsoft® SQL Server

1. Creare un nuovo database in Microsoft® SQL Server.

2. Creare un utente/accesso dedicato in Microsoft® SQL Server, mappato al database appena creato. Consentire l'accesso completo a tutti i ruoli server e database e alle autorizzazioni.

3. All'interno di GFI MailEssentials, selezionare **Creazione di rapporti > Impostazioni**.



Schermata 35: Configurazione back-end del database SQL Server

4. Selezionare **Server SQL**.

5. Selezionare **Server rilevato**, quindi scegliere dall'elenco il server SQL rilevato automaticamente. Se il server non viene rilevato, selezionare **Server specificato manualmente** e immettere l'indirizzo IP o il nome server di Microsoft® SQL Server.

6. Immettere le credenziali con autorizzazione di lettura/scrittura nel database.

7. Fare clic su **Ottieni elenco database** per estrarre l'elenco dei database dal server.

8. Dall'elenco **Database**, selezionare il database creato per Creazione di rapporti di GFI MailEssentials.

9. Fare clic su **Applica**.

Configurazione dell'eliminazione automatica del database

È possibile configurare GFI MailEssentials affinché elimini in automatico i record del database che sono anteriori a un periodo particolare.

Per impostazione predefinita, Eliminazione automatica è configurato per la cancellazione dei dati più vecchi di 12 mesi.

Per abilitare l'eliminazione automatica:

1. Selezionare **Creazione di rapporti > Impostazioni**, quindi fare clic sulla scheda **Elimina automaticamente**.

2. Selezionare **Abilita eliminazione automatica** e indicare per quanti mesi dovranno essere archiviati gli elementi nel database.

3. Fare clic su **Applica**.

> **NOTA**
> l'eliminazione automatica viene applicata solo al database corrente configurato nella scheda Creazione report.

4.2.8 Rapporto MailInsights®

MailInsights® è una funzionalità di creazione rapporti che utilizza i dati nel database di creazione rapporti per fornire informazioni relative all'utilizzo della posta elettronica e alle tendenze.

GFI MailEssentials fornisce il rapporto del Flusso di comunicazione che offre una rappresentazione grafica dei messaggi di posta scambiati tra gli utenti/gruppi selezionati e i relativi contatti. Altri rapporti di MailInsights® possono essere generati utilizzando GFI MailArchiver.

Rapporto flusso di comunicazione

Il rapporto Flusso di comunicazione mostra i primi 20 contatti con cui un utente ha comunicato nei 30 giorni precedenti.

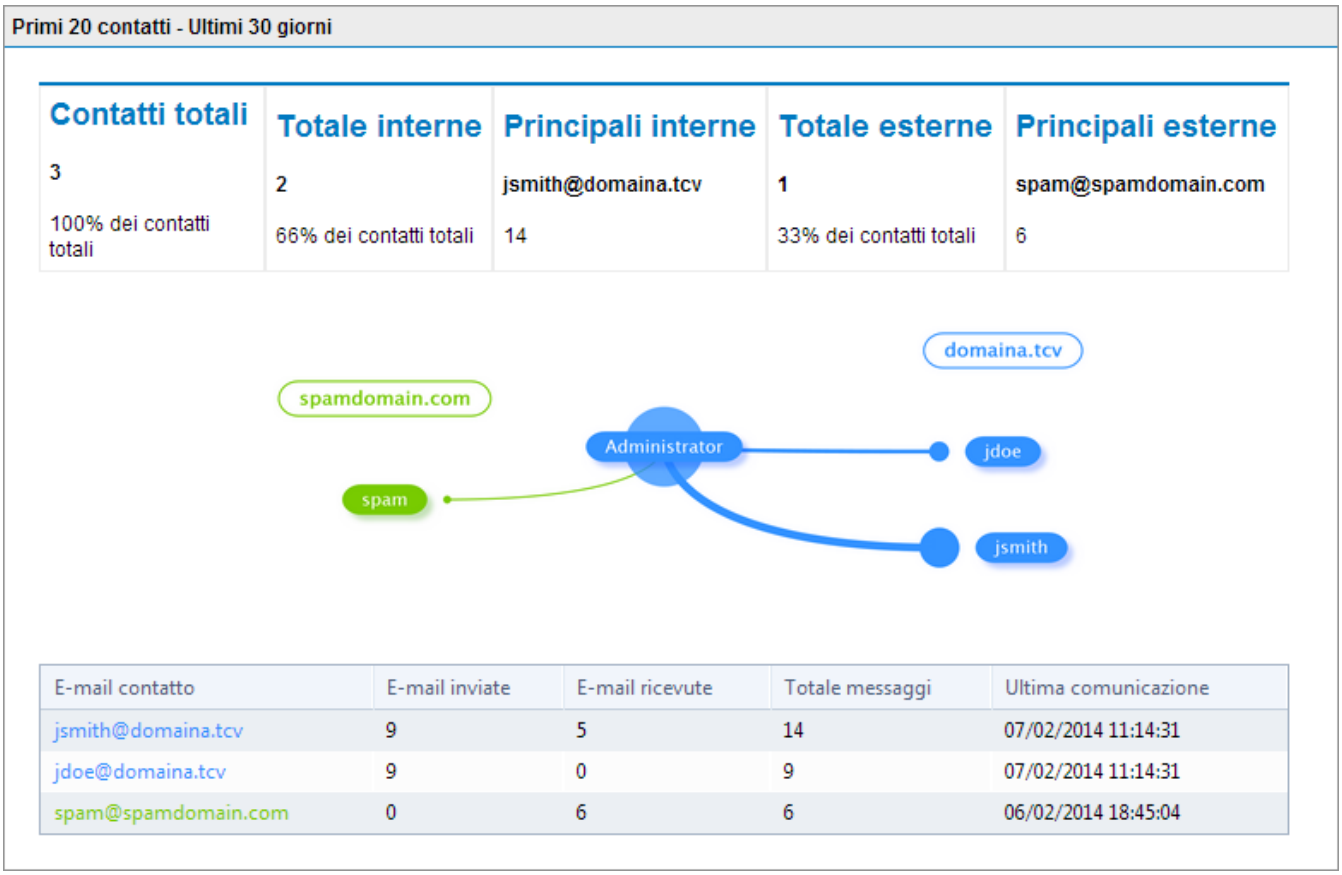
1. Selezionare **Creazione di rapporti > MailInsights**, quindi fare clic sulla scheda **Flusso di comunicazione**.

2. Gli amministratori possono generare il rapporto per qualsiasi utente di posta elettronica. Per selezionare un utente della posta elettronica, fare clic su **Cerca** quindi su **Genera** per iniziare la creazione del rapporto.

Il rapporto generato mostra i dati per l'utente selezionato come segue:

Totali	L'area principale del rapporto mostra le statistiche totali del flusso di comunicazione nei 30 giorni precedenti. » **Contatti totali**: il numero totale degli indirizzi e-mail con cui l'utente ha effettuato comunicazioni di posta elettronica. » **Totale interni**: il numero totale di utenti interni con cui l'utente ha effettuato comunicazioni. » **Principali interni**: l'indirizzo e-mail interno con cui l'utente selezionato ha comunicato di più. » **Totale esterni**: il numero totale di utenti esterni con cui l'utente ha effettuato comunicazioni. » **Principali esterni**: l'indirizzo e-mail esterno con cui l'utente selezionato ha comunicato di più.

Grafico	L'utente selezionato viene visualizzato come singola entità nel mezzo del grafico. I contatti vengono separati dai domini. Ciascun cluster di dominio viene visualizzato con un colore diverso. La larghezza del margine tra i nodi indica la forza della relazione di posta tra entità diverse.
Primi 20 contatti	I primi 20 contatti con cui ha comunicato di più l'utente selezionato. I codici colore indicano i domini dei vari contatti. La tabella indica il numero totale di messaggi inviati e ricevuti con quel contatto, insieme alla data e ora in cui si è verificata l'ultima comunicazione di posta elettronica.



Schermata 36: Rapporto flusso di comunicazione di MailInsights®

5 Sicurezza e-mail

I filtri di sicurezza di GFI MailEssentials forniscono protezione dai messaggi infetti da virus o altro tipo di messaggi dannosi.

Argomenti del presente capitolo:

5.1 Motori di scansione antivirus **74**

5.2 Protezione archivio informazioni **94**

5.3 Scanner trojan ed eseguibili **97**

5.4 Motore exploit posta **101**

5.5 Strumento di disinfezione HTML **105**

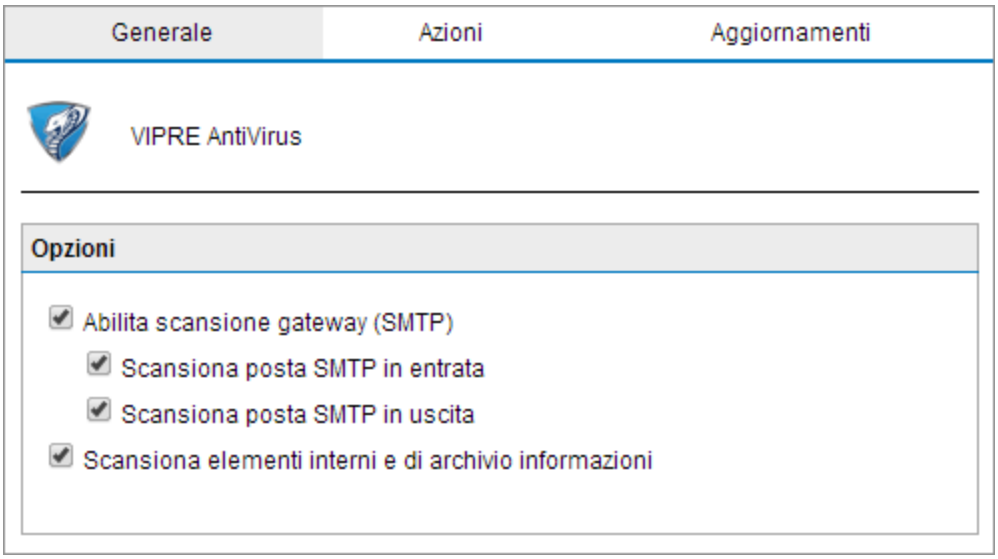
5.1 Motori di scansione antivirus

GFI MailEssentials utilizza motori antivirus multipli per la scansione di messaggi in entrata, in uscita e interni alla ricerca di virus. GFI MailEssentials viene fornito con i motori di scansione Vipre e BitDefender. È anche possibile acquistare una licenza per Kaspersky, Avira e McAfee.

Il presente capitolo illustra come configurare i motori di scansione antivirus, gli aggiornamenti, le operazioni e la sequenza di scansione.

5.1.1 Vipre

1. Selezionare **Sicurezza e-mail > Motori di scansione antivirus > Vipre**.



Schermata 37: configurazione Vipre

2. Selezionare la casella di controllo **Abilita scansione gateway (SMTP)** per scansionare i messaggi mediante questo motore di scansione antivirus.

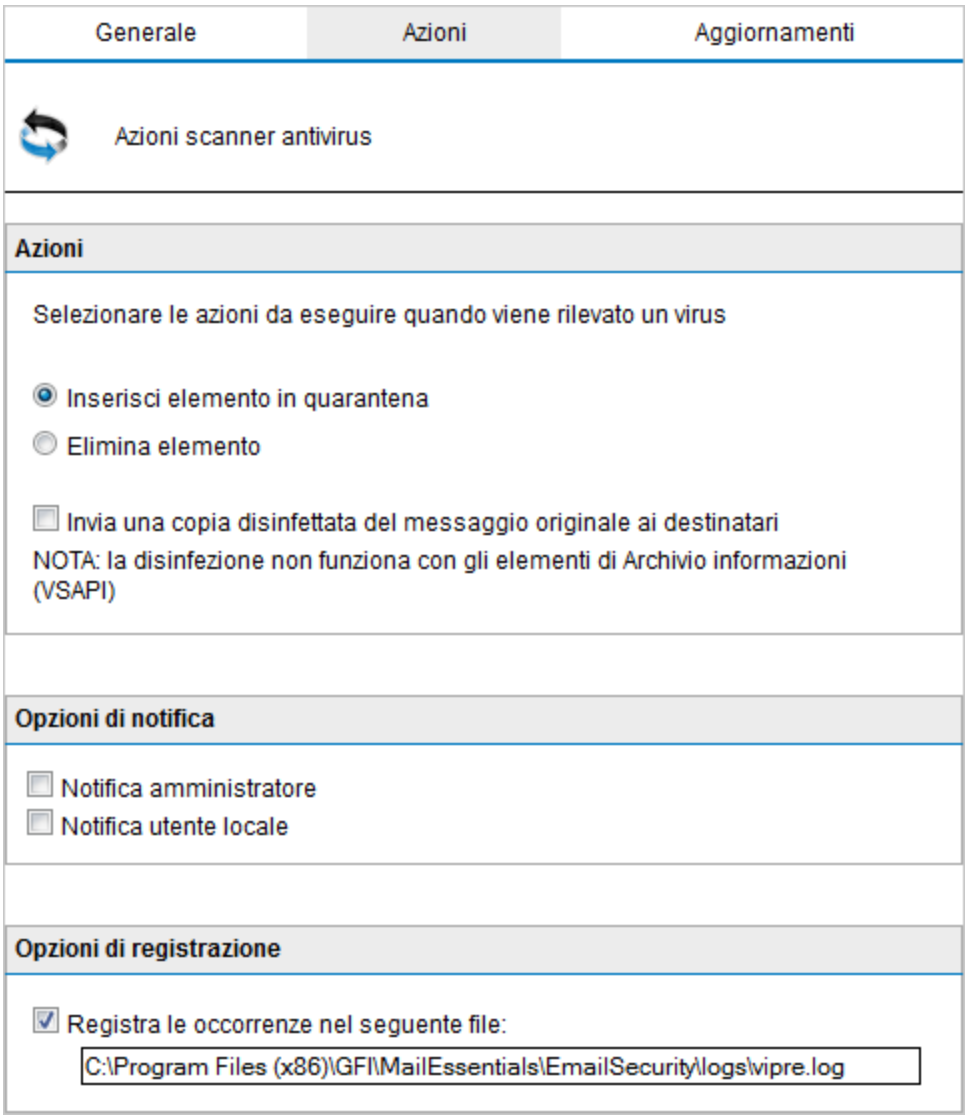
3. Scegliere se scansionare i messaggi in entrata e/o in uscita mediante il motore di scansione antivirus.

Opzione	Descrizione
Scansiona posta SMTP in entrata	Selezionare l'opzione per scansionare i messaggi in entrata.
Scansiona posta SMTP in uscita	Selezionare l'opzione per scansionare i messaggi in uscita.

4. Se si è installato GFI MailEssentials in un computer con Microsoft® Exchange è anche possibile scansionare i messaggi interni e Archivio informazioni. Selezionare **Scansiona elementi interni e di archivio informazioni**.

NOTA
Per utilizzare la funzione di Scansione antivirus archivio informazioni, è necessario abilitarla dal nodo **Protezione archivio informazioni**. Per ulteriori informazioni, fare riferimento a Protezione archivio informazioni (pagina 94).

NOTA
In questa pagina è anche possibile rivedere le informazioni di licenza e versione del motore antivirus.


Generale
Azioni
Aggiornamenti
Azioni scanner antivirus
Azioni
Selezionare le azioni da eseguire quando viene rilevato un virus
Inserisci elemento in quarantena
Elimina elemento
Invia una copia disinfettata del messaggio originale ai destinatari
NOTA: la disinfezione non funziona con gli elementi di Archivio informazioni (VSAPI)
Opzioni di notifica
Notifica amministratore
Notifica utente locale
Opzioni di registrazione
Registra le occorrenze nel seguente file:
C:\Program Files (x86)\GFI\MailEssentials\EmailSecurity\logs\vipre.log

Schermata 38: azioni motore di scansione antivirus

5. Dalla scheda **Azioni**, scegliere l'azione da effettuare quando viene bloccato un messaggio:

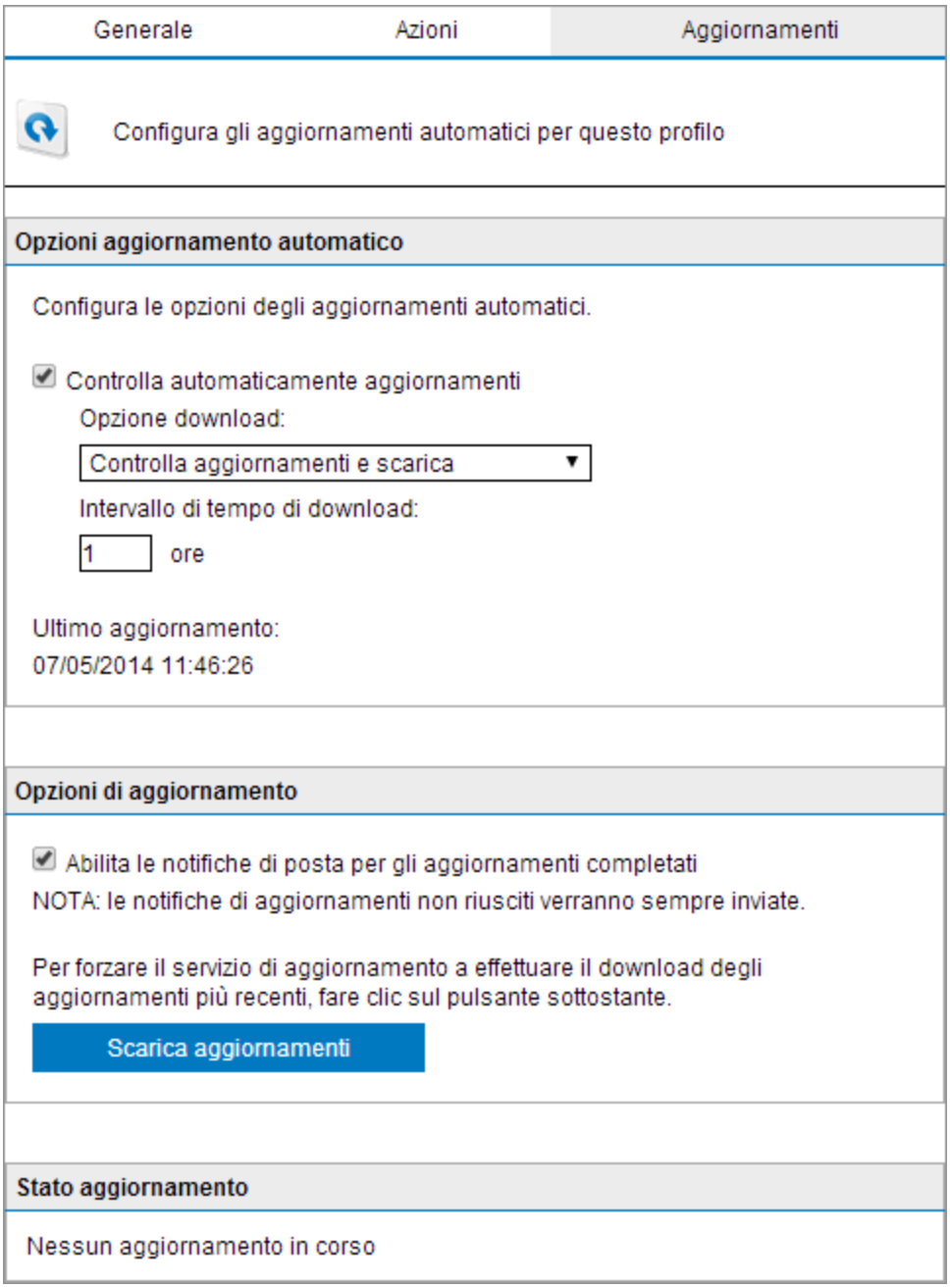
Azione	Descrizione
E-mail in quarantena	Archivia in Quarantine Store tutti i messaggi infetti rilevati dal motore antivirus selezionato. I messaggi inseriti in quarantena potranno essere successivamente rivisti (per approvazione/eliminazione). Per ulteriori informazioni, fare riferimento a Quarantena (pagina 203).
Elimina e-mail	Elimina messaggi infetti.
Invia una copia disinfettata del messaggio originale ai destinatari	Scegliere se inviare ai destinatari una copia del messaggio bloccato.

6. GFI MailEssentials può inviare notifiche di posta ogni volta che un messaggio attiva questo filtro. Per abilitare questa funzione, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Notifica amministratore	Notifica l'amministratore quando questo motore blocca un messaggio. Per ulteriori informazioni, fare riferimento a Indirizzo e-mail amministratore (pagina 241).
Notifica utente locale	Notifica il messaggio bloccato ai destinatari locali del messaggio.

7. Per registrare l'attività di questo motore in un file di registro, selezionare **Registra occorrenze nel seguente file**. Nella casella di testo, indicare il percorso e il nome del file di una posizione personalizzata su disco dove è possibile salvare il file di registro. Per impostazione predefinita, i file di registro vengono archiviati in:

<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\EmailSecurity\Logs\<nome motore>.log


Generale
Azioni
Aggiornamenti
Configura gli aggiornamenti automatici per questo profilo
Opzioni aggiornamento automatico
Configura le opzioni degli aggiornamenti automatici.
Controlla automaticamente aggiornamenti
Opzione download:
Controlla aggiornamenti e scarica
Intervallo di tempo di download:
1
ore
Ultimo aggiornamento:
07/05/2014 11:46:26
Opzioni di aggiornamento
Abilita le notifiche di posta per gli aggiornamenti completati
NOTA: le notifiche di aggiornamenti non riusciti verranno sempre inviate.
Per forzare il servizio di aggiornamento a effettuare il download degli aggiornamenti più recenti, fare clic sul pulsante sottostante.
Scarica aggiornamenti
Stato aggiornamento
Nessun aggiornamento in corso

Schermata 39: Schede Aggiornamenti motore

8. Per abilitare l'aggiornamento automatico per il del motore selezionato, dalla scheda **Aggiornamenti**, selezionare **Controlla automaticamente aggiornamenti**.

9. Dall'elenco **Opzione download**, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Controlla solo gli aggiornamenti	Selezionare questa opzione se si desidera che GFI MailEssentials controlli e notifichi solo l'amministratore quando sono disponibili aggiornamenti per il motore in questione. Questa opzione NON scaricherà automaticamente gli aggiornamenti disponibili.
Controlla aggiornamenti e scarica	Selezionare questa opzione se si desidera che GFI MailEssentials controlli e scarichi automaticamente eventuali aggiornamenti disponibili per il motore in questione.

10. Specificando un valore di intervallo in ore, indicare la frequenza con cui GFI MailEssentials deve controllare/scaricare gli aggiornamenti per questo motore.

11. Dall'area **Opzioni di aggiornamento**, selezionare **Abilita le notifiche di posta per gli aggiornamenti completati** per inviare una notifica di posta all'amministratore quando il motore si aggiorna correttamente.

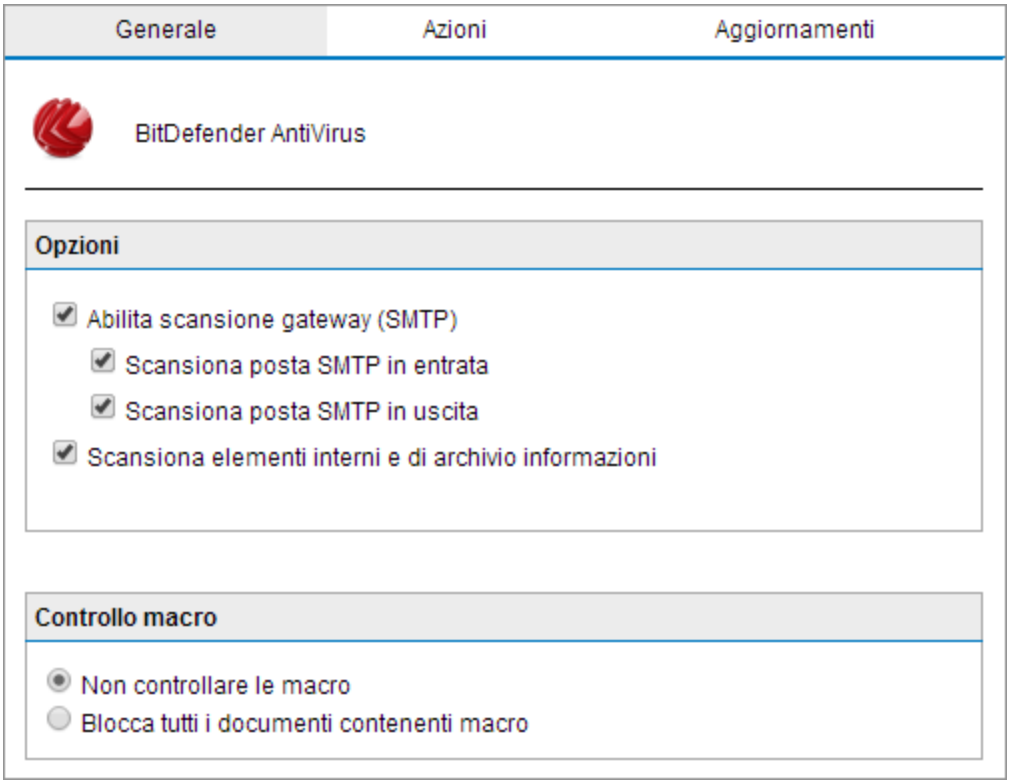
> **NOTA**
> Qualora l'aggiornamento non riuscisse, verrà sempre inviata una notifica di posta.

12. Per controllare e scaricare immediatamente gli aggiornamenti, fare clic su **Scarica aggiornamenti**.

13. Fare clic su **Applica**.

5.1.2 BitDefender

1. Selezionare **Sicurezza e-mail > Motori di scansione antivirus > BitDefender**.



Schermata 40: configurazione BitDefender

2. Selezionare la casella di controllo **Abilita scansione gateway (SMTP)** per scansionare i messaggi mediante questo motore di scansione antivirus.

3. Scegliere se scansionare i messaggi in entrata e/o in uscita mediante il motore di scansione antivirus.

Opzione	Descrizione
Scansiona posta SMTP in entrata	Selezionare l'opzione per scansionare i messaggi in entrata.
Scansiona posta SMTP in uscita	Selezionare l'opzione per scansionare i messaggi in uscita.

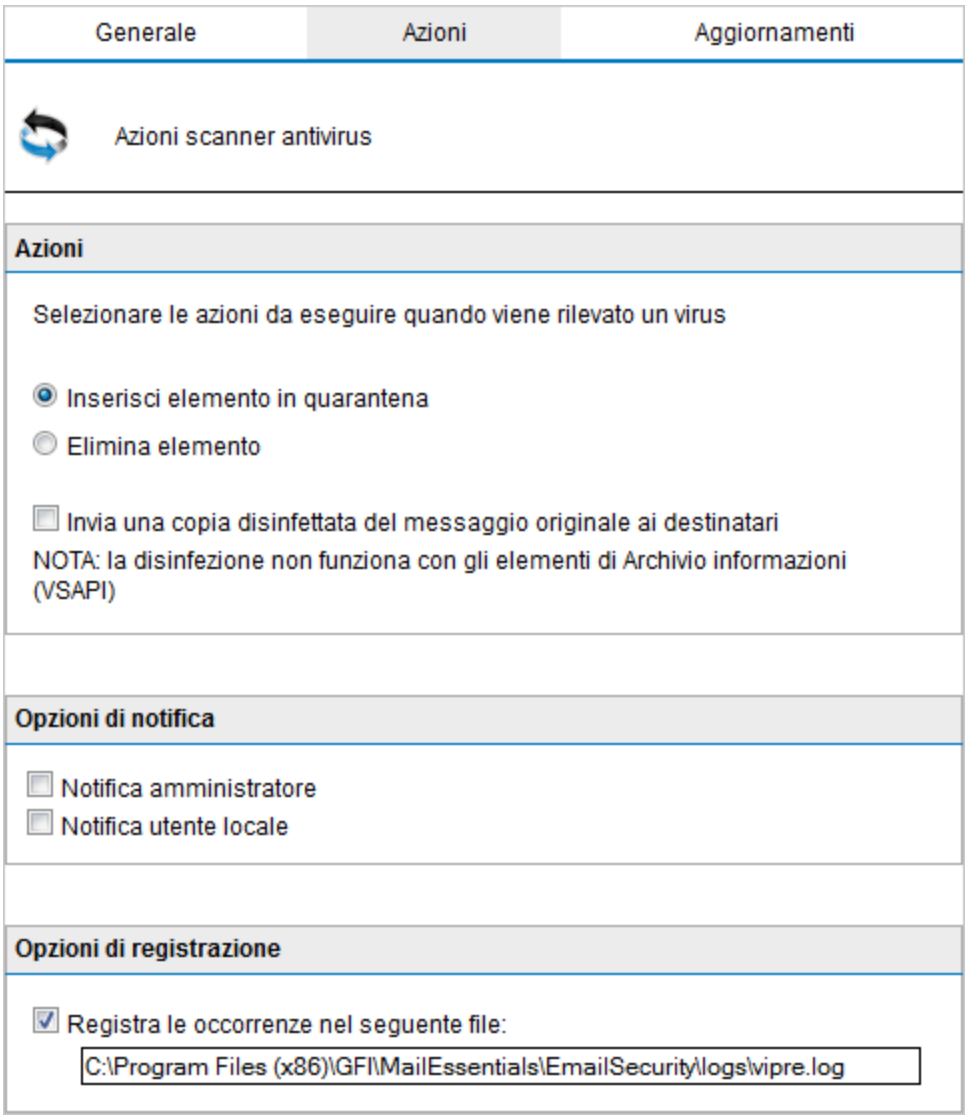
4. Se si è installato GFI MailEssentials in un computer con Microsoft® Exchange è anche possibile scansionare i messaggi interni e Archivio informazioni. Selezionare **Scansiona elementi interni e di archivio informazioni**.

> **NOTA**
> Per utilizzare la funzione di Scansione antivirus archivio informazioni, è necessario abilitarla dal nodo **Protezione archivio informazioni**. Per ulteriori informazioni, fare riferimento a Protezione archivio informazioni (pagina 94).

> **NOTA**
> In questa pagina è anche possibile rivedere le informazioni di licenza e versione del motore antivirus.

5. BitDefender può essere utilizzato anche per bloccare i messaggi con allegati contenenti macro. Per abilitare questa funzione, accedere all'area **Controllo macro** selezionando **Blocca tutti i documenti contenenti macro**.

> **NOTA**
> Se Controllo macro è disabilitato, GFI MailEssentials effettuerà comunque la scansione e il blocco dei virus macro.


Generale
Azioni
Aggiornamenti
Azioni scanner antivirus
Azioni
Selezionare le azioni da eseguire quando viene rilevato un virus
Inserisci elemento in quarantena
Elimina elemento
Invia una copia disinfettata del messaggio originale ai destinatari
NOTA: la disinfezione non funziona con gli elementi di Archivio informazioni (VSAPI)
Opzioni di notifica
Notifica amministratore
Notifica utente locale
Opzioni di registrazione
Registra le occorrenze nel seguente file:
C:\Program Files (x86)\GFI\MailEssentials\EmailSecurity\logs\vipre.log

Schermata 41: azioni motore di scansione antivirus

6. Dalla scheda **Azioni**, scegliere l'azione da effettuare quando viene bloccato un messaggio:

Azione	Descrizione
E-mail in quarantena	Archivia in Quarantine Store tutti i messaggi infetti rilevati dal motore antivirus selezionato. I messaggi inseriti in quarantena potranno essere successivamente rivisti (per approvazione/eliminazione). Per ulteriori informazioni, fare riferimento a Quarantena (pagina 203).
Elimina e-mail	Elimina messaggi infetti.
Invia una copia disinfettata del messaggio originale ai destinatari	Scegliere se inviare ai destinatari una copia del messaggio bloccato.

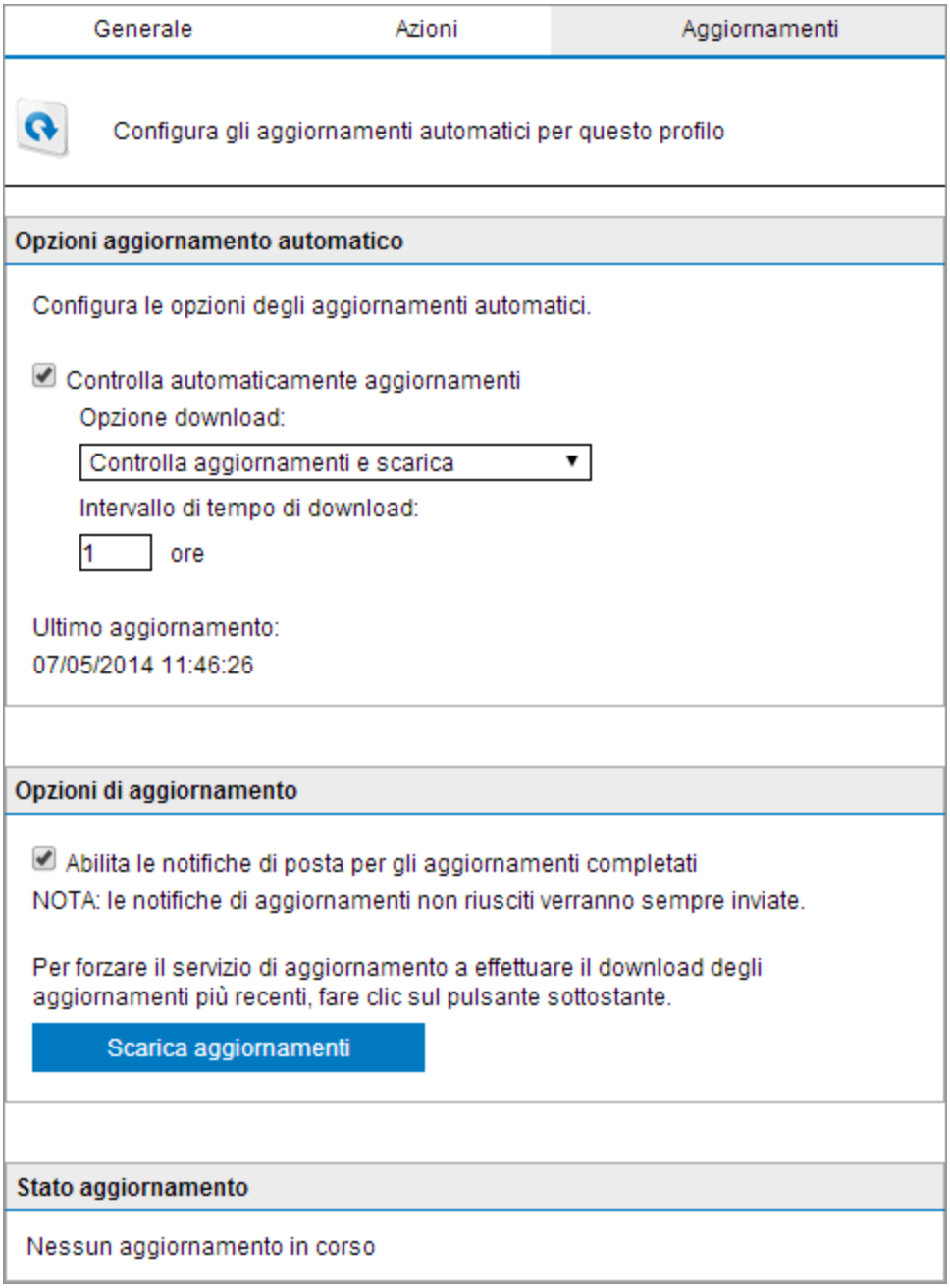
7. GFI MailEssentials può inviare notifiche di posta ogni volta che un messaggio attiva questo filtro. Per abilitare questa funzione, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Notifica amministratore	Notifica l'amministratore quando questo motore blocca un messaggio. Per ulteriori informazioni, fare riferimento a Indirizzo e-mail amministratore (pagina 241).

Opzione	Descrizione
Notifica utente locale	Notifica il messaggio bloccato ai destinatari locali del messaggio.

8. Per registrare l'attività di questo motore in un file di registro, selezionare **Registra occorrenze nel seguente file**. Nella casella di testo, indicare il percorso e il nome del file di una posizione personalizzata su disco dove è possibile salvare il file di registro. Per impostazione predefinita, i file di registro vengono archiviati in:

<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\EmailSecurity\Logs\<nome motore>.log


Generale
Azioni
Aggiornamenti
Configura gli aggiornamenti automatici per questo profilo
Opzioni aggiornamento automatico
Configura le opzioni degli aggiornamenti automatici.
Controlla automaticamente aggiornamenti
Opzione download:
Controlla aggiornamenti e scarica
Intervallo di tempo di download:
1
ore
Ultimo aggiornamento:
07/05/2014 11:46:26
Opzioni di aggiornamento
Abilita le notifiche di posta per gli aggiornamenti completati
NOTA: le notifiche di aggiornamenti non riusciti verranno sempre inviate.
Per forzare il servizio di aggiornamento a effettuare il download degli aggiornamenti più recenti, fare clic sul pulsante sottostante.
Scarica aggiornamenti
Stato aggiornamento
Nessun aggiornamento in corso

Schermata 42: Schede Aggiornamenti motore

9. Per abilitare l'aggiornamento automatico per il del motore selezionato, dalla scheda **Aggiornamenti**, selezionare **Controlla automaticamente aggiornamenti**.

10. Dall'elenco **Opzione download**, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Controlla solo gli aggiornamenti	Selezionare questa opzione se si desidera che GFI MailEssentials controlli e notifichi solo l'amministratore quando sono disponibili aggiornamenti per il motore in questione. Questa opzione NON scaricherà automaticamente gli aggiornamenti disponibili.
Controlla aggiornamenti e scarica	Selezionare questa opzione se si desidera che GFI MailEssentials controlli e scarichi automaticamente eventuali aggiornamenti disponibili per il motore in questione.

11. Specificando un valore di intervallo in ore, indicare la frequenza con cui GFI MailEssentials deve controllare/scaricare gli aggiornamenti per questo motore.

12. Dall'area **Opzioni di aggiornamento**, selezionare **Abilita le notifiche di posta per gli aggiornamenti completati** per inviare una notifica di posta all'amministratore quando il motore si aggiorna correttamente.

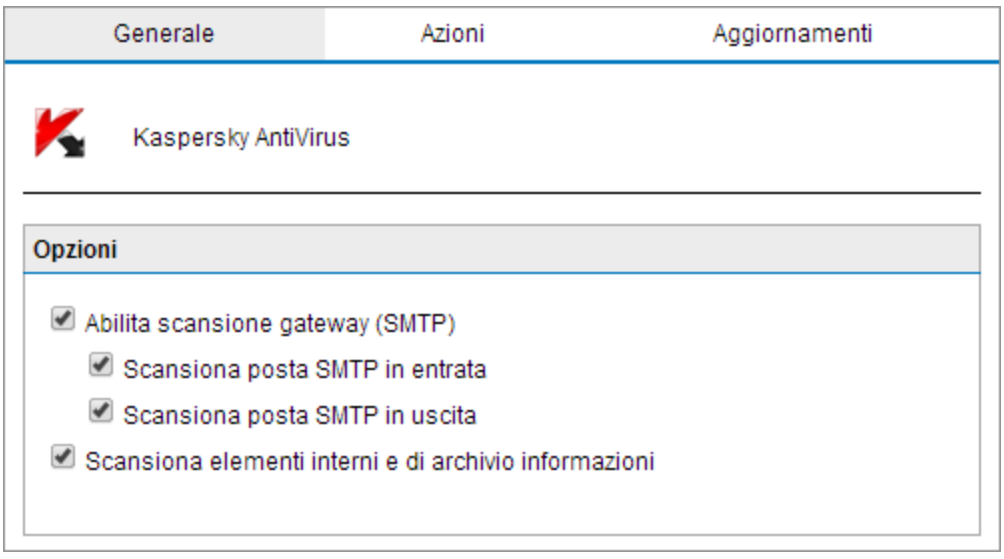
> **NOTA**
> Qualora l'aggiornamento non riuscisse, verrà sempre inviata una notifica di posta.

13. Per controllare e scaricare immediatamente gli aggiornamenti, fare clic su **Scarica aggiornamenti**.

14. Fare clic su **Applica**.

5.1.3 Kaspersky

1. Selezionare **Sicurezza e-mail > Motori di scansione antivirus > Kaspersky**.



Schermata 43: configurazione Kaspersky

2. Selezionare la casella di controllo **Abilita scansione gateway (SMTP)** per scansionare i messaggi mediante questo motore di scansione antivirus.

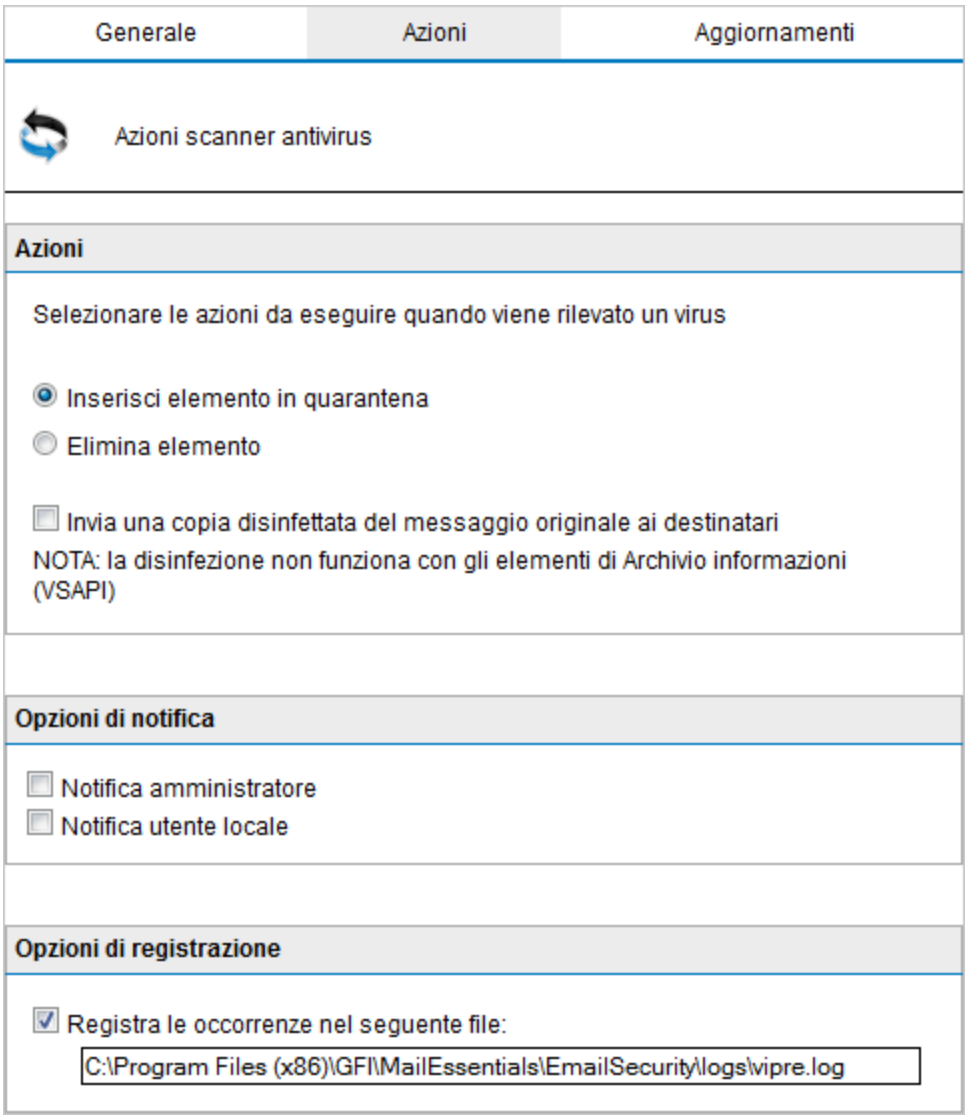
3. Scegliere se scansionare i messaggi in entrata e/o in uscita mediante il motore di scansione antivirus.

Opzione	Descrizione
Scansiona posta SMTP in entrata	Selezionare l'opzione per scansionare i messaggi in entrata.
Scansiona posta SMTP in uscita	Selezionare l'opzione per scansionare i messaggi in uscita.

4. Se si è installato GFI MailEssentials in un computer con Microsoft® Exchange è anche possibile scansionare i messaggi interni e Archivio informazioni. Selezionare **Scansiona elementi interni e di archivio informazioni**.

> **NOTA**
> Per utilizzare la funzione di Scansione antivirus archivio informazioni, è necessario abilitarla dal nodo **Protezione archivio informazioni**. Per ulteriori informazioni, fare riferimento a Protezione archivio informazioni (pagina 94).

> **NOTA**
> In questa pagina è anche possibile rivedere le informazioni di licenza e versione del motore antivirus.


Generale
Azioni
Aggiornamenti
Azioni scanner antivirus
Azioni
Selezionare le azioni da eseguire quando viene rilevato un virus
Inserisci elemento in quarantena
Elimina elemento
Invia una copia disinfettata del messaggio originale ai destinatari
NOTA: la disinfezione non funziona con gli elementi di Archivio informazioni (VSAPI)
Opzioni di notifica
Notifica amministratore
Notifica utente locale
Opzioni di registrazione
Registra le occorrenze nel seguente file:
C:\Program Files (x86)\GFI\MailEssentials\EmailSecurity\logs\vipre.log

Schermata 44: azioni motore di scansione antivirus

5. Dalla scheda **Azioni**, scegliere l'azione da effettuare quando viene bloccato un messaggio:

Azione	Descrizione
E-mail in quarantena	Archivia in Quarantine Store tutti i messaggi infetti rilevati dal motore antivirus selezionato. I messaggi inseriti in quarantena potranno essere successivamente rivisti (per approvazione/eliminazione). Per ulteriori informazioni, fare riferimento a Quarantena (pagina 203).
Elimina e-mail	Elimina messaggi infetti.
Invia una copia disinfettata del messaggio originale ai destinatari	Scegliere se inviare ai destinatari una copia del messaggio bloccato.

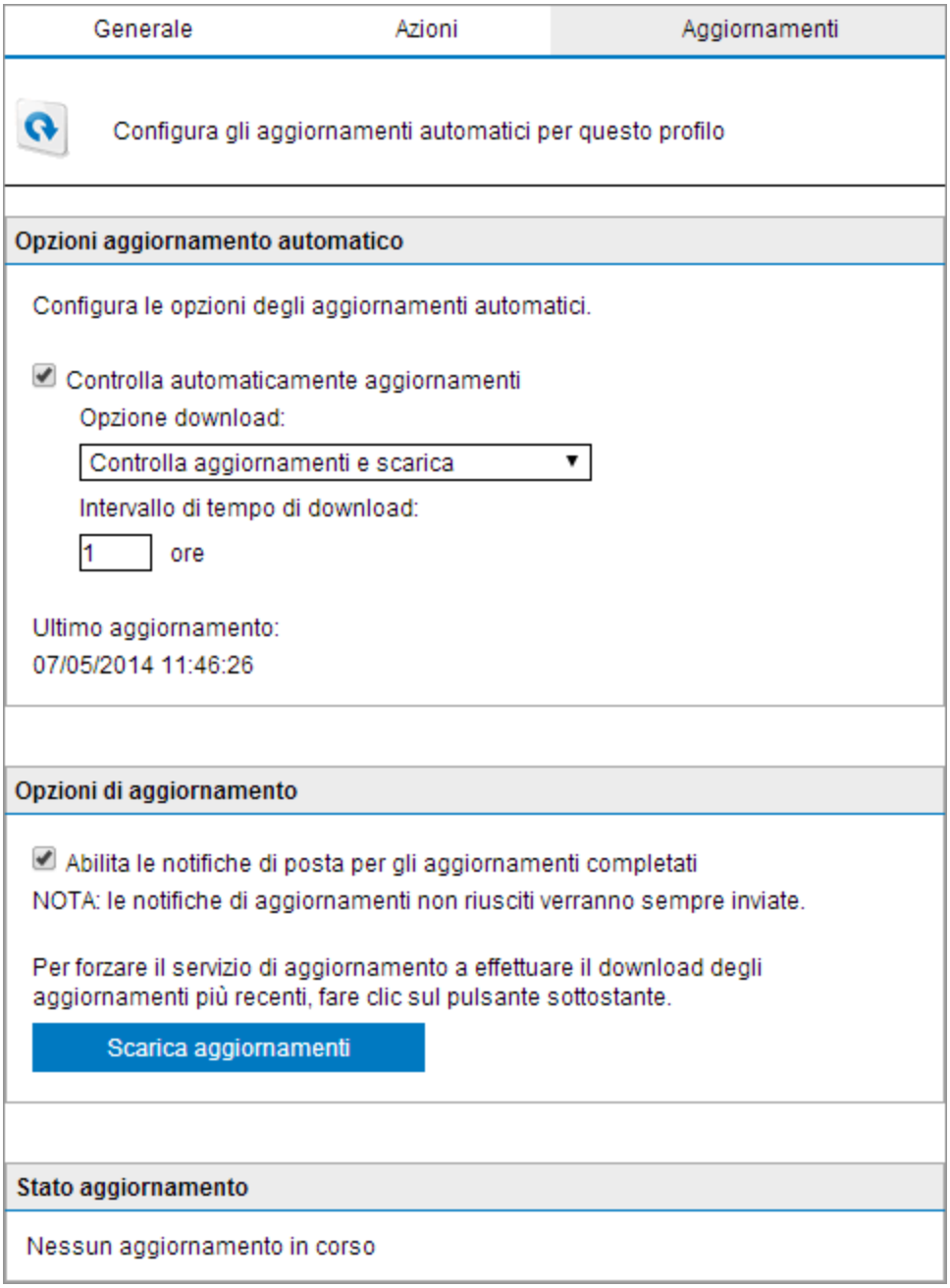
6. GFI MailEssentials può inviare notifiche di posta ogni volta che un messaggio attiva questo filtro. Per abilitare questa funzione, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Notifica amministratore	Notifica l'amministratore quando questo motore blocca un messaggio. Per ulteriori informazioni, fare riferimento a Indirizzo e-mail amministratore (pagina 241).

Opzione	Descrizione
Notifica utente locale	Notifica il messaggio bloccato ai destinatari locali del messaggio.

7. Per registrare l'attività di questo motore in un file di registro, selezionare **Registra occorrenze nel seguente file**. Nella casella di testo, indicare il percorso e il nome del file di una posizione personalizzata su disco dove è possibile salvare il file di registro. Per impostazione predefinita, i file di registro vengono archiviati in:

<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\EmailSecurity\Logs\<nome motore>.log


Generale
Azioni
Aggiornamenti
Configura gli aggiornamenti automatici per questo profilo
Opzioni aggiornamento automatico
Configura le opzioni degli aggiornamenti automatici.
Controlla automaticamente aggiornamenti
Opzione download:
Controlla aggiornamenti e scarica
Intervallo di tempo di download:
1
ore
Ultimo aggiornamento:
07/05/2014 11:46:26
Opzioni di aggiornamento
Abilita le notifiche di posta per gli aggiornamenti completati
NOTA: le notifiche di aggiornamenti non riusciti verranno sempre inviate.
Per forzare il servizio di aggiornamento a effettuare il download degli aggiornamenti più recenti, fare clic sul pulsante sottostante.
Scarica aggiornamenti
Stato aggiornamento
Nessun aggiornamento in corso

Schermata 45: Schede Aggiornamenti motore

8. Per abilitare l'aggiornamento automatico per il del motore selezionato, dalla scheda **Aggiornamenti**, selezionare **Controlla automaticamente aggiornamenti**.

9. Dall'elenco **Opzione download**, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Controlla solo gli aggiornamenti	Selezionare questa opzione se si desidera che GFI MailEssentials controlli e notifichi solo l'amministratore quando sono disponibili aggiornamenti per il motore in questione. Questa opzione NON scaricherà automaticamente gli aggiornamenti disponibili.
Controlla aggiornamenti e scarica	Selezionare questa opzione se si desidera che GFI MailEssentials controlli e scarichi automaticamente eventuali aggiornamenti disponibili per il motore in questione.

10. Specificando un valore di intervallo in ore, indicare la frequenza con cui GFI MailEssentials deve controllare/scaricare gli aggiornamenti per questo motore.

11. Dall'area **Opzioni di aggiornamento**, selezionare **Abilita le notifiche di posta per gli aggiornamenti completati** per inviare una notifica di posta all'amministratore quando il motore si aggiorna correttamente.

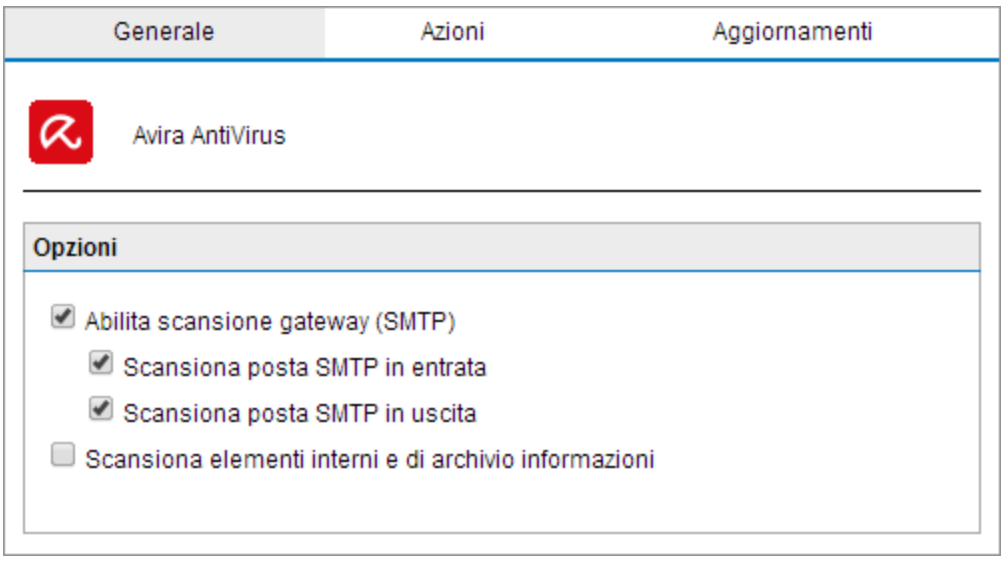
> **NOTA**
> Qualora l'aggiornamento non riuscisse, verrà sempre inviata una notifica di posta.

12. Per controllare e scaricare immediatamente gli aggiornamenti, fare clic su **Scarica aggiornamenti**.

13. Fare clic su **Applica**.

5.1.4 Avira

1. Selezionare **Sicurezza e-mail > Motori di scansione antivirus > Avira**.



Schermata 46: Configurazione di Avira

2. Selezionare la casella di controllo **Abilita scansione gateway (SMTP)** per scansionare i messaggi mediante questo motore di scansione antivirus.

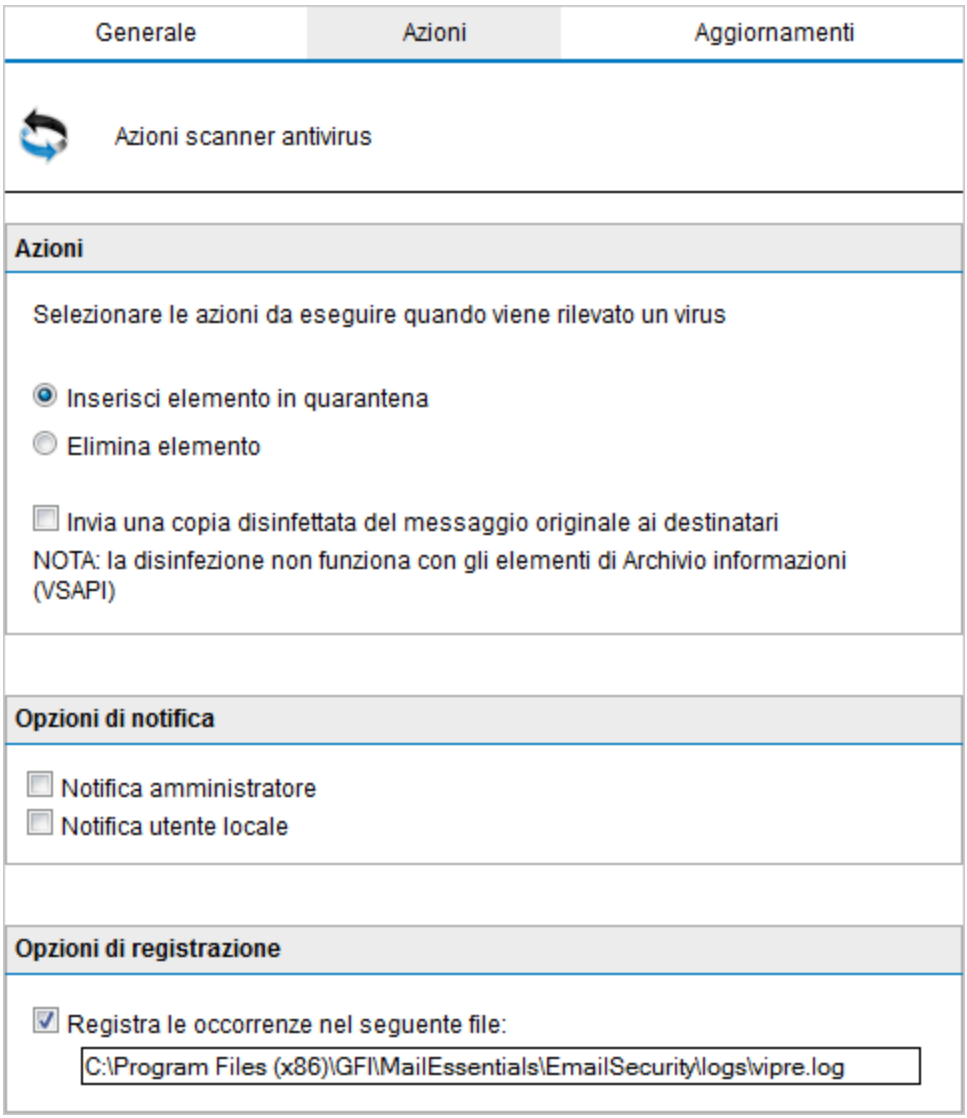
3. Scegliere se scansionare i messaggi in entrata e/o in uscita mediante il motore di scansione antivirus.

Opzione	Descrizione
Scansiona posta SMTP in entrata	Selezionare l'opzione per scansionare i messaggi in entrata.
Scansiona posta SMTP in uscita	Selezionare l'opzione per scansionare i messaggi in uscita.

4. Se si è installato GFI MailEssentials in un computer con Microsoft® Exchange è anche possibile scansionare i messaggi interni e Archivio informazioni. Selezionare **Scansiona elementi interni e di archivio informazioni**.

NOTA
Per utilizzare la funzione di Scansione antivirus archivio informazioni, è necessario abilitarla dal nodo **Protezione archivio informazioni**. Per ulteriori informazioni, fare riferimento a Protezione archivio informazioni (pagina 94).

NOTA
In questa pagina è anche possibile rivedere le informazioni di licenza e versione del motore antivirus.


Generale
Azioni
Aggiornamenti
Azioni scanner antivirus
Azioni
Selezionare le azioni da eseguire quando viene rilevato un virus
Inserisci elemento in quarantena
Elimina elemento
Invia una copia disinfettata del messaggio originale ai destinatari
NOTA: la disinfezione non funziona con gli elementi di Archivio informazioni (VSAPI)
Opzioni di notifica
Notifica amministratore
Notifica utente locale
Opzioni di registrazione
Registra le occorrenze nel seguente file:
C:\Program Files (x86)\GFI\MailEssentials\EmailSecurity\logs\vipre.log

Schermata 47: azioni motore di scansione antivirus

5. Dalla scheda **Azioni**, scegliere l'azione da effettuare quando viene bloccato un messaggio:

Azione	Descrizione
E-mail in quarantena	Archivia in Quarantine Store tutti i messaggi infetti rilevati dal motore antivirus selezionato. I messaggi inseriti in quarantena potranno essere successivamente rivisti (per approvazione/eliminazione). Per ulteriori informazioni, fare riferimento a Quarantena (pagina 203).
Elimina e-mail	Elimina messaggi infetti.
Invia una copia disinfettata del messaggio originale ai destinatari	Scegliere se inviare ai destinatari una copia del messaggio bloccato.

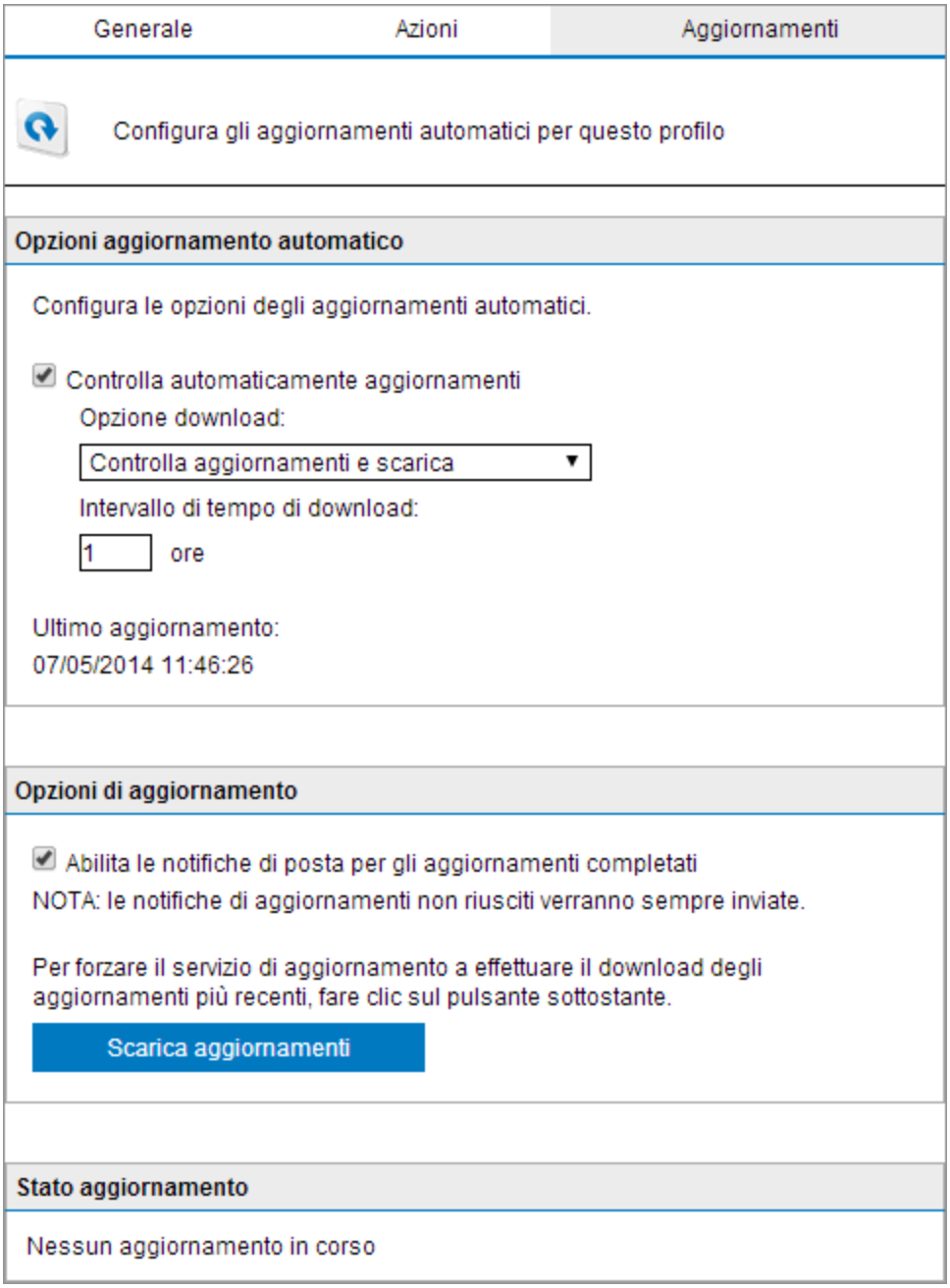
6. GFI MailEssentials può inviare notifiche di posta ogni volta che un messaggio attiva questo filtro. Per abilitare questa funzione, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Notifica amministratore	Notifica l'amministratore quando questo motore blocca un messaggio. Per ulteriori informazioni, fare riferimento a Indirizzo e-mail amministratore (pagina 241).

Opzione	Descrizione
Notifica utente locale	Notifica il messaggio bloccato ai destinatari locali del messaggio.

7. Per registrare l'attività di questo motore in un file di registro, selezionare **Registra occorrenze nel seguente file**. Nella casella di testo, indicare il percorso e il nome del file di una posizione personalizzata su disco dove è possibile salvare il file di registro. Per impostazione predefinita, i file di registro vengono archiviati in:

<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\EmailSecurity\Logs\<nome motore>.log


Generale
Azioni
Aggiornamenti
Configura gli aggiornamenti automatici per questo profilo
Opzioni aggiornamento automatico
Configura le opzioni degli aggiornamenti automatici.
Controlla automaticamente aggiornamenti
Opzione download:
Controlla aggiornamenti e scarica
Intervallo di tempo di download:
1
ore
Ultimo aggiornamento:
07/05/2014 11:46:26
Opzioni di aggiornamento
Abilita le notifiche di posta per gli aggiornamenti completati
NOTA: le notifiche di aggiornamenti non riusciti verranno sempre inviate.
Per forzare il servizio di aggiornamento a effettuare il download degli aggiornamenti più recenti, fare clic sul pulsante sottostante.
Scarica aggiornamenti
Stato aggiornamento
Nessun aggiornamento in corso

Schermata 48: Schede Aggiornamenti motore

8. Per abilitare l'aggiornamento automatico per il del motore selezionato, dalla scheda **Aggiornamenti**, selezionare **Controlla automaticamente aggiornamenti**.

9. Dall'elenco **Opzione download**, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Controlla solo gli aggiornamenti	Selezionare questa opzione se si desidera che GFI MailEssentials controlli e notifichi solo l'amministratore quando sono disponibili aggiornamenti per il motore in questione. Questa opzione NON scaricherà automaticamente gli aggiornamenti disponibili.
Controlla aggiornamenti e scarica	Selezionare questa opzione se si desidera che GFI MailEssentials controlli e scarichi automaticamente eventuali aggiornamenti disponibili per il motore in questione.

10. Specificando un valore di intervallo in ore, indicare la frequenza con cui GFI MailEssentials deve controllare/scaricare gli aggiornamenti per questo motore.

11. Dall'area **Opzioni di aggiornamento**, selezionare **Abilita le notifiche di posta per gli aggiornamenti completati** per inviare una notifica di posta all'amministratore quando il motore si aggiorna correttamente.

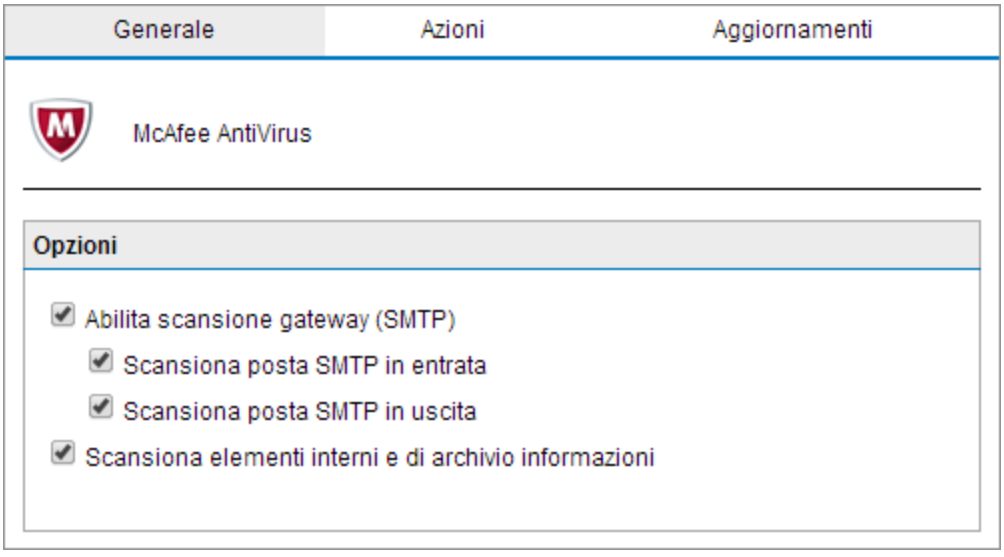
> **NOTA**
> Qualora l'aggiornamento non riuscisse, verrà sempre inviata una notifica di posta.

12. Per controllare e scaricare immediatamente gli aggiornamenti, fare clic su **Scarica aggiornamenti**.

13. Fare clic su **Applica**.

5.1.5 McAfee

1. Selezionare **Sicurezza e-mail > Motori di scansione antivirus > McAfee**.



Schermata 49: configurazione McAfee

2. Selezionare la casella di controllo **Abilita scansione gateway (SMTP)** per scansionare i messaggi mediante questo motore di scansione antivirus.

3. Scegliere se scansionare i messaggi in entrata e/o in uscita mediante il motore di scansione antivirus.

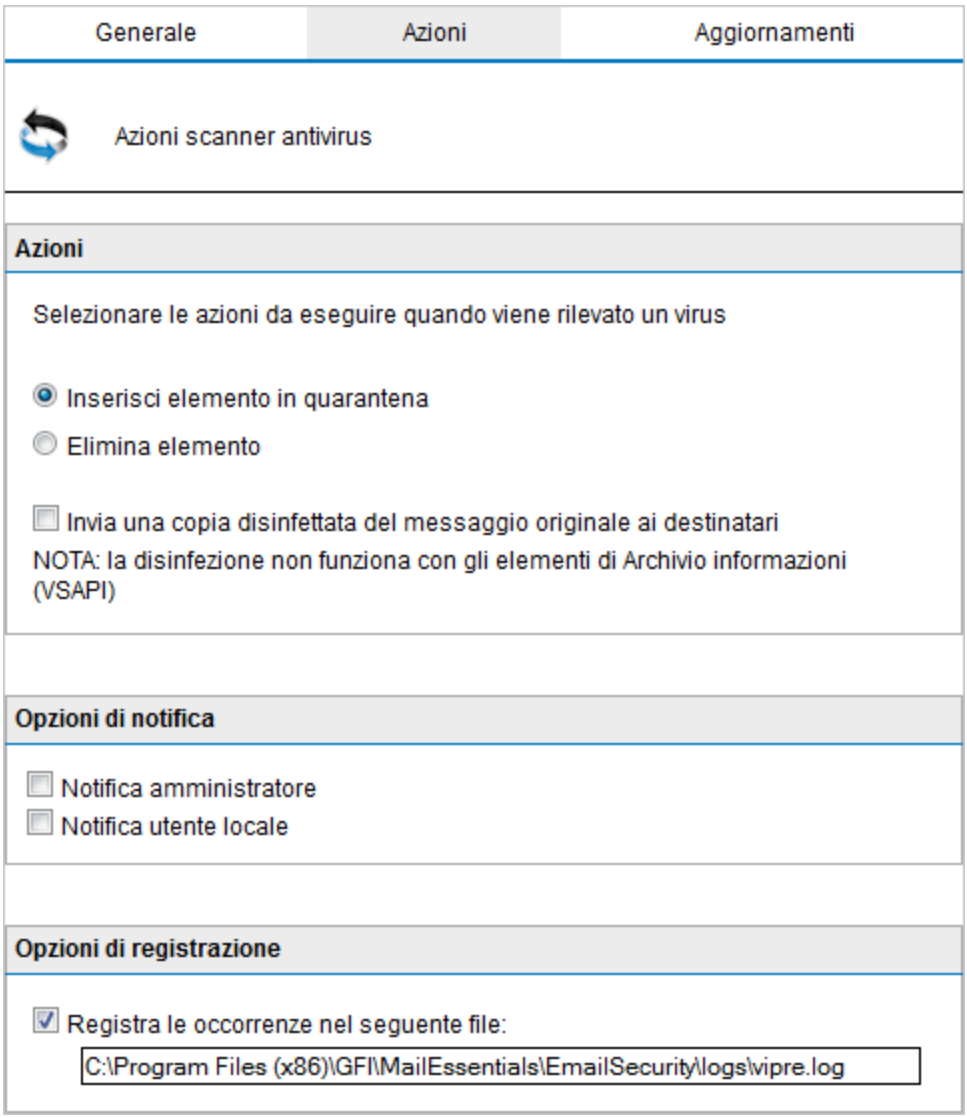
Opzione	Descrizione
Scansiona posta SMTP in entrata	Selezionare l'opzione per scansionare i messaggi in entrata.
Scansiona posta SMTP in uscita	Selezionare l'opzione per scansionare i messaggi in uscita.

4. Se si è installato GFI MailEssentials in un computer con Microsoft® Exchange è anche possibile scansionare i messaggi interni e Archivio informazioni. Selezionare **Scansiona elementi interni e di archivio informazioni**.

> **NOTA**
> Per utilizzare la funzione di Scansione antivirus archivio informazioni, è necessario abilitarla dal nodo **Protezione archivio informazioni**. Per ulteriori informazioni, fare riferimento a Protezione archivio informazioni (pagina 94).

> **NOTA**
> In questa pagina è anche possibile rivedere le informazioni di licenza e versione del motore antivirus.

5. McAfee Antivirus può essere utilizzato anche per bloccare i messaggi con allegati contenenti macro. Per abilitare questa funzione, accedere all'area **Controllo macro** selezionando **Blocca tutti i documenti contenenti macro**.


Generale
Azioni
Aggiornamenti
Azioni scanner antivirus
Azioni
Selezionare le azioni da eseguire quando viene rilevato un virus
Inserisci elemento in quarantena
Elimina elemento
Invia una copia disinfettata del messaggio originale ai destinatari
NOTA: la disinfezione non funziona con gli elementi di Archivio informazioni (VSAPI)
Opzioni di notifica
Notifica amministratore
Notifica utente locale
Opzioni di registrazione
Registra le occorrenze nel seguente file:
C:\Program Files (x86)\GFI\MailEssentials\EmailSecurity\logs\vipre.log

Schermata 50: azioni motore di scansione antivirus

6. Dalla scheda **Azioni**, scegliere l'azione da effettuare quando viene bloccato un messaggio:

Azione	Descrizione
E-mail in quarantena	Archivia in Quarantine Store tutti i messaggi infetti rilevati dal motore antivirus selezionato. I messaggi inseriti in quarantena potranno essere successivamente rivisti (per approvazione/eliminazione). Per ulteriori informazioni, fare riferimento a Quarantena (pagina 203).
Elimina e-mail	Elimina messaggi infetti.
Invia una copia disinfettata del messaggio originale ai destinatari	Scegliere se inviare ai destinatari una copia del messaggio bloccato.

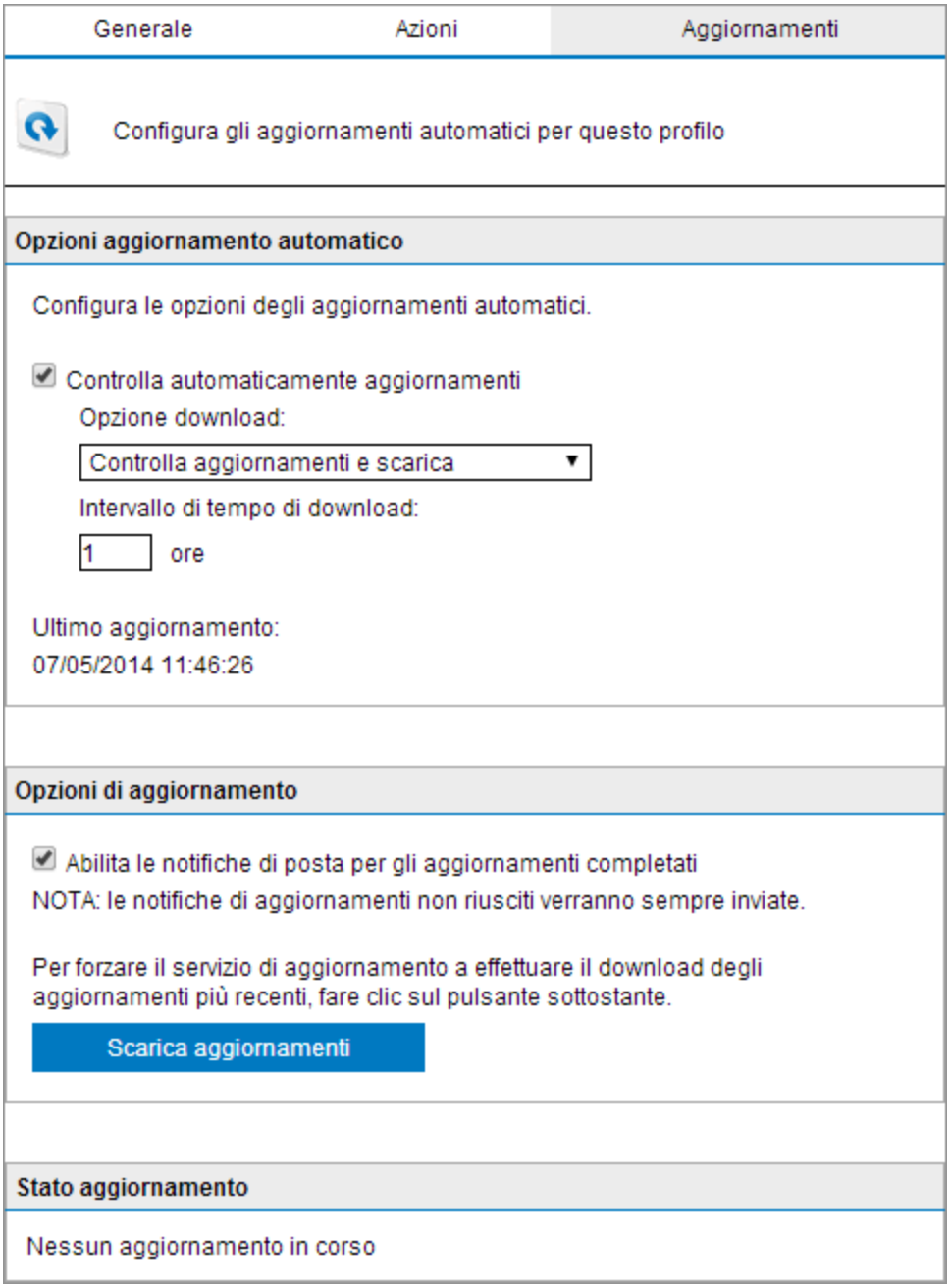
7. GFI MailEssentials può inviare notifiche di posta ogni volta che un messaggio attiva questo filtro. Per abilitare questa funzione, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Notifica amministratore	Notifica l'amministratore quando questo motore blocca un messaggio. Per ulteriori informazioni, fare riferimento a Indirizzo e-mail amministratore (pagina 241).

Opzione	Descrizione
Notifica utente locale	Notifica il messaggio bloccato ai destinatari locali del messaggio.

8. Per registrare l'attività di questo motore in un file di registro, selezionare **Registra occorrenze nel seguente file**. Nella casella di testo, indicare il percorso e il nome del file di una posizione personalizzata su disco dove è possibile salvare il file di registro. Per impostazione predefinita, i file di registro vengono archiviati in:

<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\EmailSecurity\Logs\<nome motore>.log


Generale
Azioni
Aggiornamenti
Configura gli aggiornamenti automatici per questo profilo
Opzioni aggiornamento automatico
Configura le opzioni degli aggiornamenti automatici.
Controlla automaticamente aggiornamenti
Opzione download:
Controlla aggiornamenti e scarica
Intervallo di tempo di download:
1
ore
Ultimo aggiornamento:
07/05/2014 11:46:26
Opzioni di aggiornamento
Abilita le notifiche di posta per gli aggiornamenti completati
NOTA: le notifiche di aggiornamenti non riusciti verranno sempre inviate.
Per forzare il servizio di aggiornamento a effettuare il download degli aggiornamenti più recenti, fare clic sul pulsante sottostante.
Scarica aggiornamenti
Stato aggiornamento
Nessun aggiornamento in corso

Schermata 51: Schede Aggiornamenti motore

9. Per abilitare l'aggiornamento automatico per il del motore selezionato, dalla scheda **Aggiornamenti**, selezionare **Controlla automaticamente aggiornamenti**.

10. Dall'elenco **Opzione download**, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Controlla solo gli aggiornamenti	Selezionare questa opzione se si desidera che GFI MailEssentials controlli e notifichi solo l'amministratore quando sono disponibili aggiornamenti per il motore in questione. Questa opzione NON scaricherà automaticamente gli aggiornamenti disponibili.
Controlla aggiornamenti e scarica	Selezionare questa opzione se si desidera che GFI MailEssentials controlli e scarichi automaticamente eventuali aggiornamenti disponibili per il motore in questione.

11. Specificando un valore di intervallo in ore, indicare la frequenza con cui GFI MailEssentials deve controllare/scaricare gli aggiornamenti per questo motore.

12. Dall'area **Opzioni di aggiornamento**, selezionare **Abilita le notifiche di posta per gli aggiornamenti completati** per inviare una notifica di posta all'amministratore quando il motore si aggiorna correttamente.

> **NOTA**
> Qualora l'aggiornamento non riuscisse, verrà sempre inviata una notifica di posta.

13. Per controllare e scaricare immediatamente gli aggiornamenti, fare clic su **Scarica aggiornamenti**.

14. Fare clic su **Applica**.

5.2 Protezione archivio informazioni

Quando GFI MailEssentials è installato su un computer con Microsoft® Exchange server, Protezione archivio informazioni consente l'utilizzo dei motori di scansione antivirus per eseguire la scansione di Archivio informazioni di Microsoft® Exchange alla ricerca di virus.

> **NOTA**
> Quando GFI MailEssentials è installato su un computer Microsoft® Exchange Server 2007/2010, Protezione archivio informazioni è disponibile solo se sono installati i ruoli Server cassetta postale e Trasporto hub.

> **NOTA**
> Information Store Protection (VSAPI) non è supportato su Microsoft® Exchange Server 2013, in quanto VSAPI è stato rimosso da Microsoft® Exchange Server 2013.

La presente sezione illustrerà all'utente come abilitare la Scansione archivio informazioni e in che modo scegliere il metodo di scansione utilizzato da VSAPI (Virus Scanning API).

5.2.1 Scansione archivio informazioni

1. Selezionare **Sicurezza e-mail > Protezione archivio informazioni**.

Schermata 52: nodo Protezione archivio informazioni

2. Dalla scheda **Scansione antivirus archivio informazioni**, selezionare **Abilita scansione antivirus archivio informazioni**.

3. Fare clic su **Applica**.

Lo stato dei motori di scansione antivirus utilizzati per scansionare archivio informazioni è riportato nella tabella.

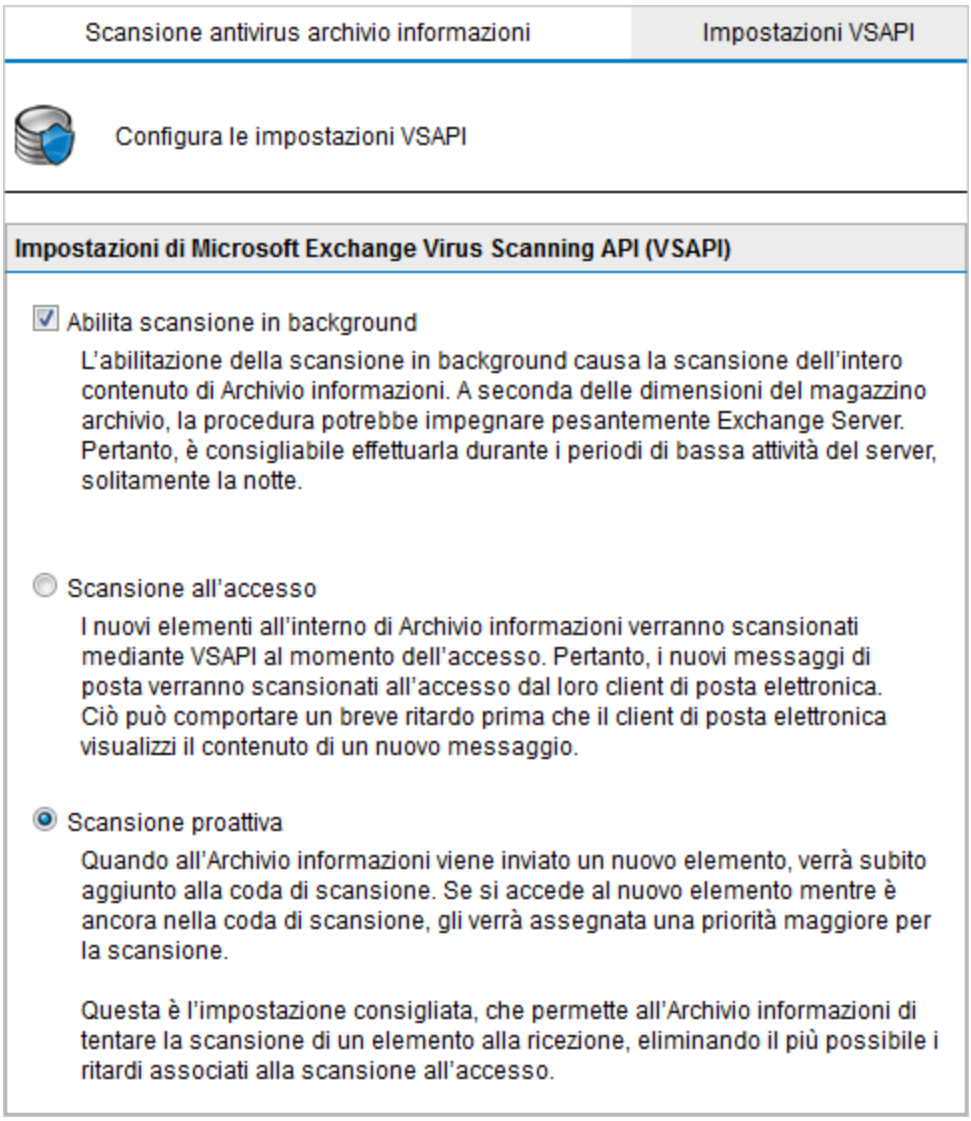
È anche possibile disabilitare un motore antivirus specifico da Scansione archivio informazioni. Andare alla pagina Motori di scansione antivirus, selezionare il motore antivirus e disabilitare **Scansiona elementi interni e di archivio informazioni**.

5.2.2 Impostazioni VSAPI

Il metodo utilizzato da GFI MailEssentials per l'accesso a messaggi e allaegati in Archivio informazioni di Microsoft® Exchange è VSAPI (Virus Scanning Application Programming Interface). GFI MailEssentials consente di indicare il metodo da utilizzare per la scansione di archivio informazioni.

1. Selezionare **Sicurezza e-mail > Protezione archivio informazioni**.

2. Selezionare la scheda **Impostazioni VSAPI**.


Scansione antivirus archivio informazioni
Impostazioni VSAPI
Configura le impostazioni VSAPI
Impostazioni di Microsoft Exchange Virus Scanning API (VSAPI)
Abilita scansione in background
L'abilitazione della scansione in background causa la scansione dell'intero contenuto di Archivio informazioni. A seconda delle dimensioni del magazzino archivio, la procedura potrebbe impegnare pesantemente Exchange Server. Pertanto, è consigliabile effettuarla durante i periodi di bassa attività del server, solitamente la notte.
Scansione all'accesso
I nuovi elementi all'interno di Archivio informazioni verranno scansionati mediante VSAPI al momento dell'accesso. Pertanto, i nuovi messaggi di posta verranno scansionati all'accesso dal loro client di posta elettronica. Ciò può comportare un breve ritardo prima che il client di posta elettronica visualizzi il contenuto di un nuovo messaggio.
Scansione proattiva
Quando all'Archivio informazioni viene inviato un nuovo elemento, verrà subito aggiunto alla coda di scansione. Se si accede al nuovo elemento mentre è ancora nella coda di scansione, gli verrà assegnata una priorità maggiore per la scansione.
Questa è l'impostazione consigliata, che permette all'Archivio informazioni di tentare la scansione di un elemento alla ricezione, eliminando il più possibile i ritardi associati alla scansione all'accesso.

Schermata 53: Impostazioni VSAPI

3. (Facoltativo) Per eseguire la scansione in background di archivio informazioni, selezionare **Abilita scansione in background**.

AVVISO
L'abilitazione della scansione in background causa la scansione dell'intero contenuto di Archivio informazioni. Ciò può portare a un elevato carico di elaborazione sul server Microsoft® Exchange, a seconda della quantità di elementi salvati in Archivio informazioni. È consigliabile abilitare questa opzione solo nei periodi di bassa attività del server, come la notte.

4. Selezionare un metodo di scansione VSAPI:

Metodo di scansione	Descrizione
Scansione all'accesso	I nuovi elementi all'interno di Archivio informazioni verranno scansionati al momento in cui vi accede il client di posta. Ciò può comportare un breve ritardo prima che il client di posta elettronica visualizzi il contenuto di un nuovo messaggio.

Metodo di scansione	Descrizione
Scansione proattiva	I nuovi elementi aggiunti all'Archivio informazioni vengono aggiunti a una coda per essere sottoposti a scansione. Questa è la procedura predefinita e consigliata, dato che, di norma, si evita il ritardo associato alla scansione all'accesso. **NOTA** Qualora un client di posta elettronica tenti di accedere a un elemento che si trova ancora nella coda, gli verrà allocata una priorità di scansione superiore per permetterne la scansione immediata.

5. Fare clic su **Applica**.

5.3 Scanner trojan ed eseguibili

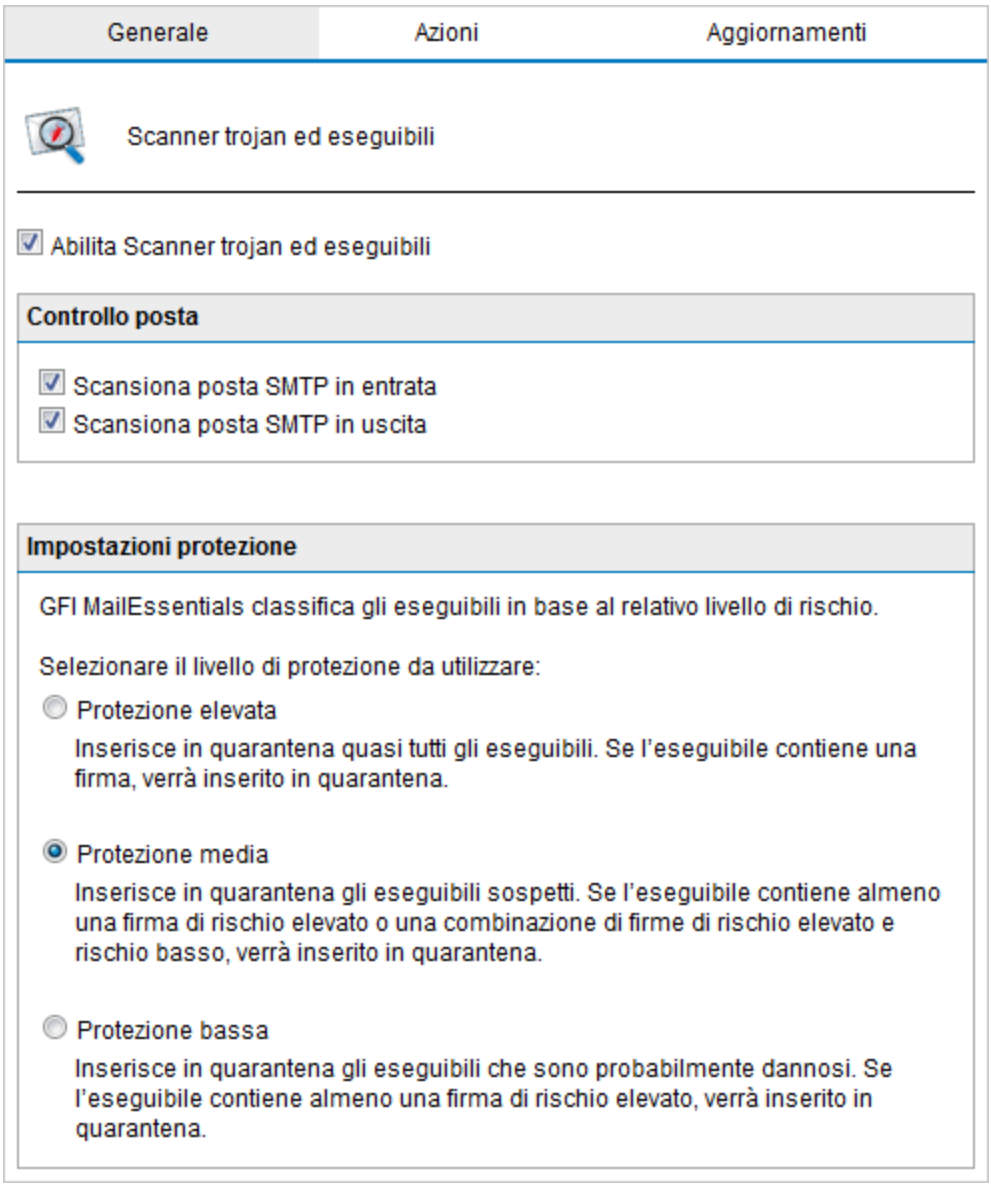
Scanner trojan ed eseguibili analizza e determina la funzione dei file eseguibili allegati ai messaggi. Questo scanner può successivamente inserire in quarantena qualsiasi eseguibile dall'attività sospetta, come i trojan.

Funzionamento scanner trojan ed eseguibili

GFI MailEssentials valuta il livello di rischio di un file eseguibile effettuando la decompilazione dell'eseguibile e rilevando in tempo reale le operazioni che potrebbe eseguire. Di conseguenza, confronta le funzionalità dell'eseguibile con un database di azioni dannose e valuta in tal modo il livello di rischio del file. Lo scanner trojan ed eseguibili consente la rilevazione e blocco di trojan potenzialmente dannosi, sconosciuti o occasionali, prima che compromettano la rete dell'utente.

5.3.1 Configurazione scanner trojan ed eseguibili

1. Selezionare **Sicurezza e-mail > Scanner trojan ed eseguibili**.


Generale
Azioni
Aggiornamenti
Scanner trojan ed eseguibili
Abilita Scanner trojan ed eseguibili
Controllo posta
Scansiona posta SMTP in entrata
Scansiona posta SMTP in uscita
Impostazioni protezione
GFI MailEssentials classifica gli eseguibili in base al relativo livello di rischio.
Selezionare il livello di protezione da utilizzare:
Protezione elevata
Inserisce in quarantena quasi tutti gli eseguibili. Se l'eseguibile contiene una firma, verrà inserito in quarantena.
Protezione media
Inserisce in quarantena gli eseguibili sospetti. Se l'eseguibile contiene almeno una firma di rischio elevato o una combinazione di firme di rischio elevato e rischio basso, verrà inserito in quarantena.
Protezione bassa
Inserisce in quarantena gli eseguibili che sono probabilmente dannosi. Se l'eseguibile contiene almeno una firma di rischio elevato, verrà inserito in quarantena.

Schermata 54: scanner trojan ed eseguibili: scheda Generale

2. Per attivare il filtro, selezionare **Abilita Scanner trojan ed eseguibili**.

3. Nell'area **Controllo posta**, indicare i messaggi da controllare alla ricerca di trojan e altri eseguibili dannosi facendo clic su:

Opzione	Descrizione
Controlla messaggi di posta in arrivo	Scansiona i messaggi in entrata alla ricerca di trojan e file eseguibili dannosi.
Controlla messaggi di posta in uscita	Scansiona i messaggi in uscita alla ricerca di trojan e file eseguibili dannosi.

4. Dall'area **Impostazioni protezione**, scegliere il livello di protezione richiesto:

Livello di protezione	Descrizione
Protezione elevata	Blocca tutti gli eseguibili che contengono firme dannose note.
Protezione media	Blocca eseguibili sospetti. I messaggi vengono bloccati se l'eseguibile contiene almeno una firma di rischio elevato o una combinazione di firme di rischio elevato e rischio basso.

Livello di protezione	Descrizione
Protezione bassa	Blocca solo gli eseguibili dannosi. I messaggi vengono bloccati se l'eseguibile contiene almeno una firma di rischio elevato.

5. Dalla scheda **Azioni**, configurare le azioni che si desidera far eseguire a GFI MailEssentials sui messaggi che contengono un eseguibile dannoso.

> **NOTA**
> I messaggi bloccati dallo scanner trojan ed eseguibili vengono sempre inseriti in quarantena.

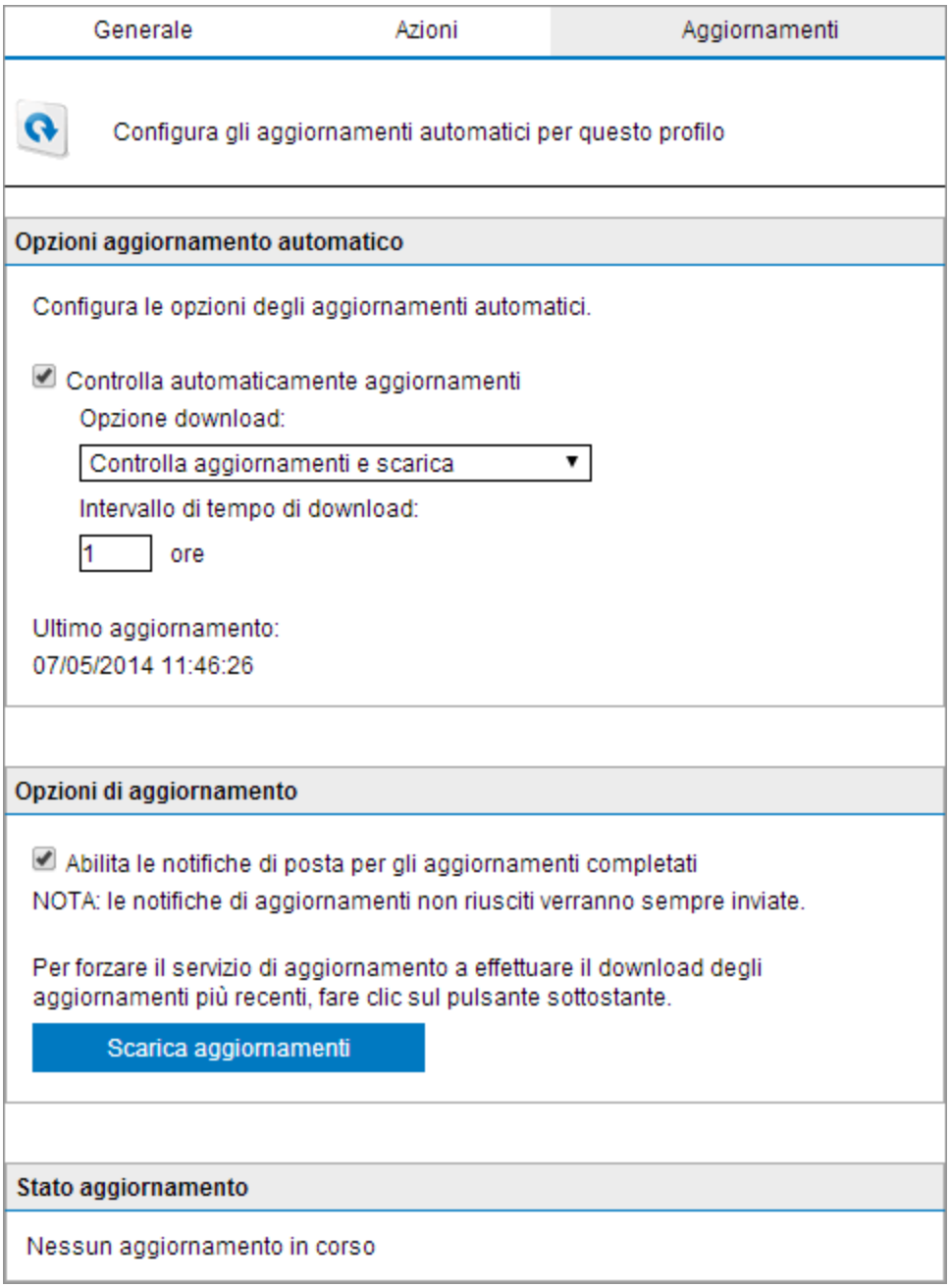
> **NOTA**
> Quando GFI MailEssentials viene installato sullo stesso computer di Microsoft® Exchange 2003, GFI MailEssentials potrebbe non riuscire a bloccare i messaggi in uscita ma invece sostituire il contenuto bloccato con un rapporto sulle minacce.

6. GFI MailEssentials può inviare notifiche di posta ogni volta che un messaggio attiva questo filtro. Per abilitare questa funzione, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Notifica amministratore	Notifica l'amministratore quando questo motore blocca un messaggio. Per ulteriori informazioni, fare riferimento a Indirizzo e-mail amministratore (pagina 241).
Notifica utente locale	Notifica il messaggio bloccato ai destinatari locali del messaggio.

7. Per registrare l'attività di questo motore in un file di registro, selezionare **Registra occorrenze nel seguente file**. Nella casella di testo, indicare il percorso e il nome del file di una posizione personalizzata su disco dove è possibile salvare il file di registro. Per impostazione predefinita, i file di registro vengono archiviati in:

```
<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\EmailSecurity\Logs\<nome motore>.log
```


Generale
Azioni
Aggiornamenti
Configura gli aggiornamenti automatici per questo profilo
Opzioni aggiornamento automatico
Configura le opzioni degli aggiornamenti automatici.
Controlla automaticamente aggiornamenti
Opzione download:
Controlla aggiornamenti e scarica
Intervallo di tempo di download:
1
ore
Ultimo aggiornamento:
07/05/2014 11:46:26
Opzioni di aggiornamento
Abilita le notifiche di posta per gli aggiornamenti completati
NOTA: le notifiche di aggiornamenti non riusciti verranno sempre inviate.
Per forzare il servizio di aggiornamento a effettuare il download degli aggiornamenti più recenti, fare clic sul pulsante sottostante.
Scarica aggiornamenti
Stato aggiornamento
Nessun aggiornamento in corso

Schermata 55: Schede Aggiornamenti motore

8. Per abilitare l'aggiornamento automatico per il del motore selezionato, dalla scheda **Aggiornamenti**, selezionare **Controlla automaticamente aggiornamenti**.

9. Dall'elenco **Opzione download**, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Controlla solo gli aggiornamenti	Selezionare questa opzione se si desidera che GFI MailEssentials controlli e notifichi solo l'amministratore quando sono disponibili aggiornamenti per il motore in questione. Questa opzione NON scaricherà automaticamente gli aggiornamenti disponibili.
Controlla aggiornamenti e scarica	Selezionare questa opzione se si desidera che GFI MailEssentials controlli e scarichi automaticamente eventuali aggiornamenti disponibili per il motore in questione.

10. Specificando un valore di intervallo in ore, indicare la frequenza con cui GFI MailEssentials deve controllare/scaricare gli aggiornamenti per questo motore.

11. Dall'area **Opzioni di aggiornamento**, selezionare **Abilita le notifiche di posta per gli aggiornamenti completati** per inviare una notifica di posta all'amministratore quando il motore si aggiorna correttamente.

> **NOTA**
> Qualora l'aggiornamento non riuscisse, verrà sempre inviata una notifica di posta.

12. Per controllare e scaricare immediatamente gli aggiornamenti, fare clic su **Scarica aggiornamenti**.

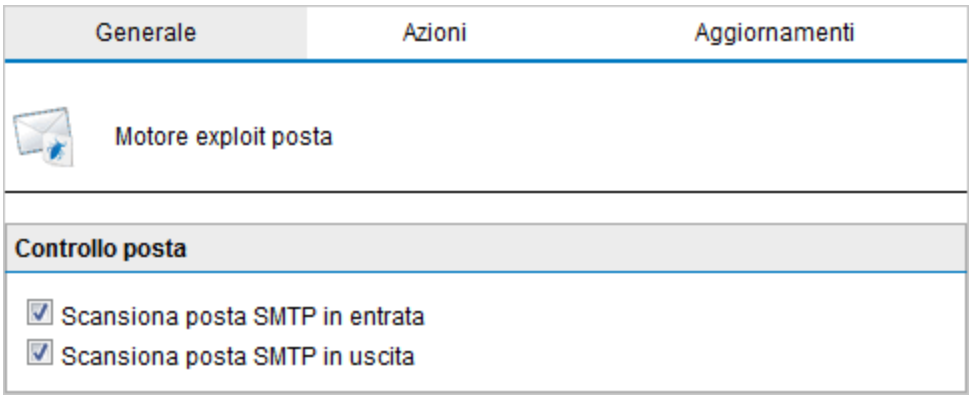
13. Fare clic su **Applica**.

5.4 Motore exploit posta

Motore exploit posta blocca gli exploit integrati nel messaggio che potrebbero essere eseguiti sul computer del destinatario al momento dell'apertura o ricezione del messaggio. Un exploit sfrutta le vulnerabilità note delle applicazioni e dei sistemi operativi allo scopo di compromettere la sicurezza del sistema. Ad esempio, esegue un programma o un comando oppure installa una backdoor.

5.4.1 Configurazione motore exploit posta

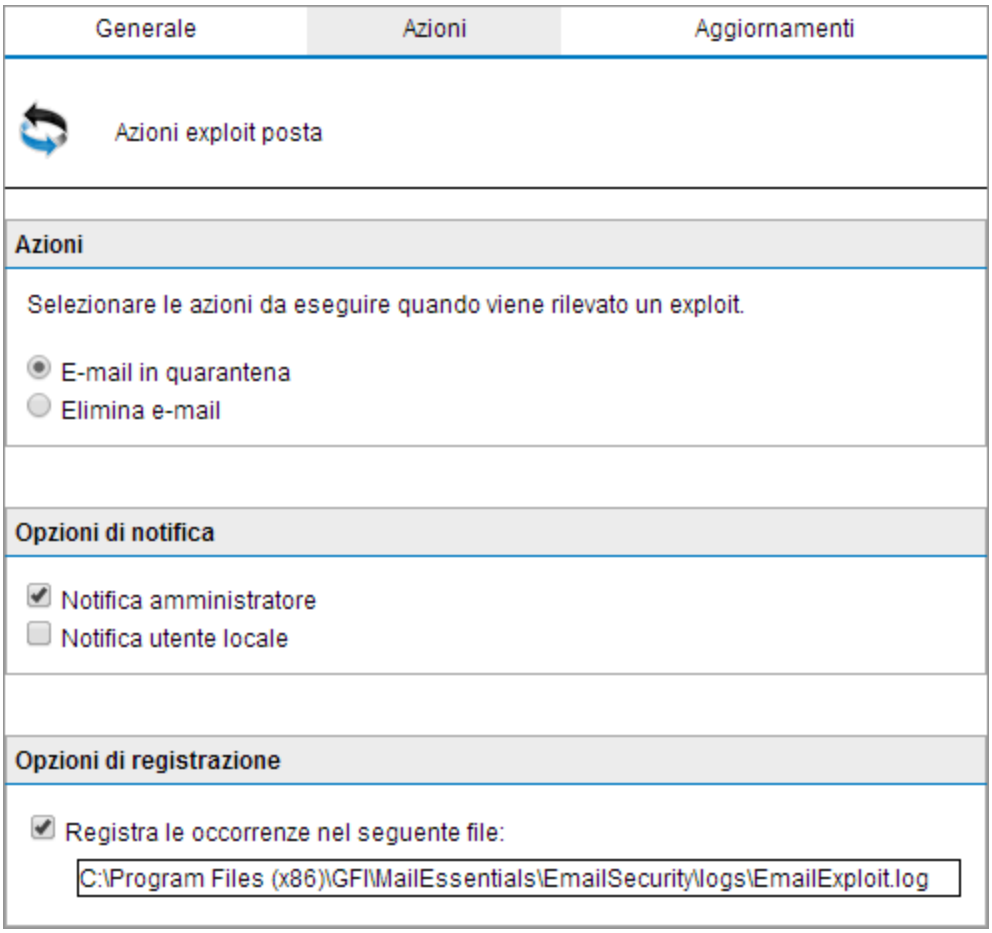
1. Selezionare **Sicurezza e-mail > Motore exploit posta**.



Schermata 56: configurazione exploit posta

2. Dalla scheda **Generale**, selezionare se scansionare i messaggi in entrata e/o in uscita.

Opzione	Descrizione
Scansiona posta SMTP in entrata	Selezionare l'opzione per scansionare i messaggi in entrata.
Scansiona posta SMTP in uscita	Selezionare l'opzione per scansionare i messaggi in uscita.



Schermata 57: Azioni exploit posta

3. Dalla scheda **Azioni**, scegliere l'azione da effettuare quando viene bloccato un messaggio:

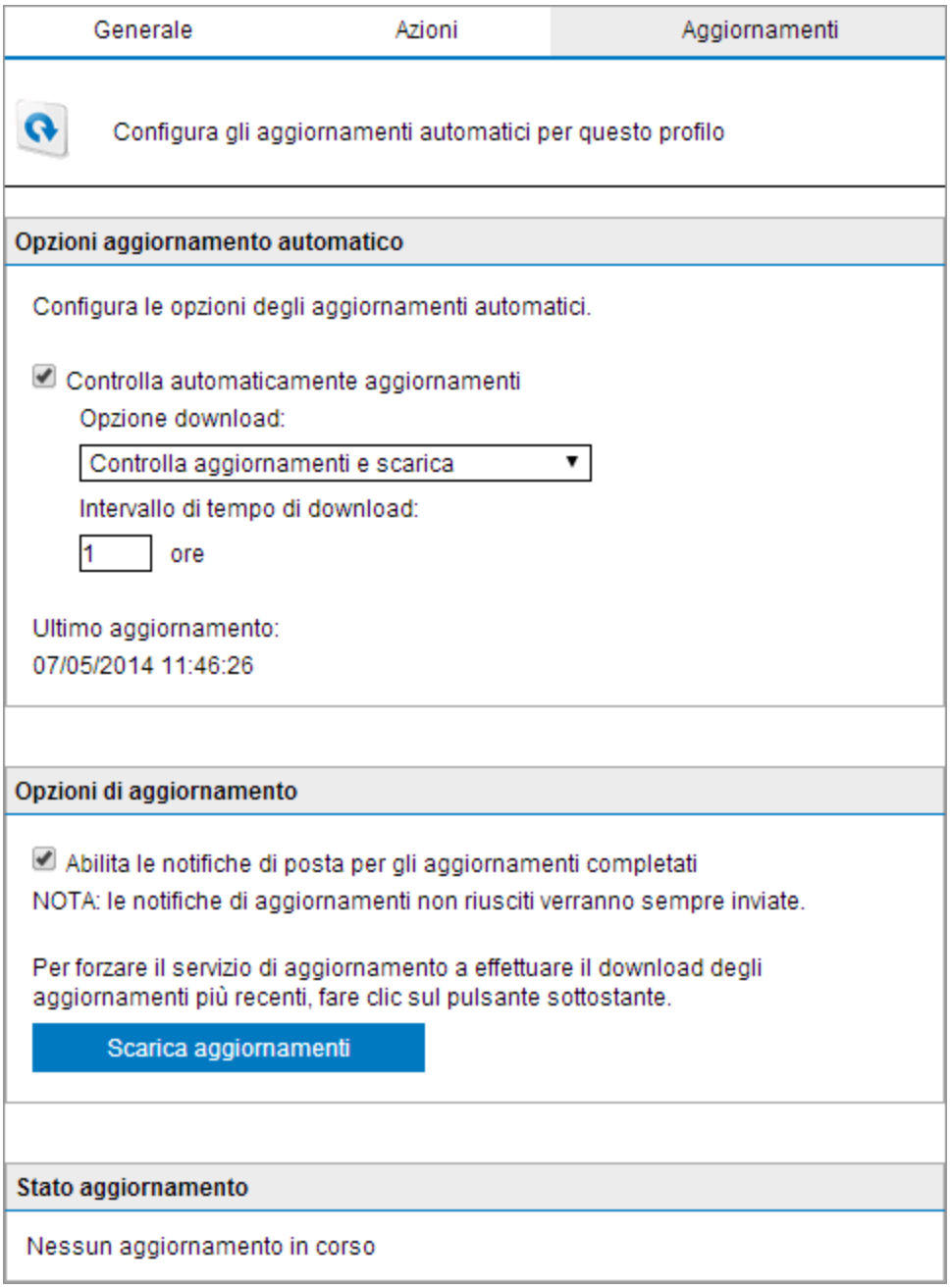
Azione	Descrizione
Inserisci elemento in quarantena	Archivia in Quarantine Store tutti i messaggi infetti rilevati dal motore exploit posta. I messaggi inseriti in quarantena potranno essere successivamente rivisti (per approvazione/eliminazione). Per ulteriori informazioni, fare riferimento a Operazioni con i messaggi messi in quarantena (pagina 213).
Elimina elemento	Elimina messaggi infetti.

4. GFI MailEssentials può inviare notifiche di posta ogni volta che un messaggio attiva questo filtro. Per abilitare questa funzione, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Notifica amministratore	Notifica l'amministratore quando questo motore blocca un messaggio. Per ulteriori informazioni, fare riferimento a Indirizzo e-mail amministratore (pagina 241).
Notifica utente locale	Notifica il messaggio bloccato ai destinatari locali del messaggio.

5. Per registrare l'attività di questo motore in un file di registro, selezionare **Registra occorrenze nel seguente file**. Nella casella di testo, indicare il percorso e il nome del file di una posizione personalizzata su disco dove è possibile salvare il file di registro. Per impostazione predefinita, i file di registro vengono archiviati in:

<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\EmailSecurity\Logs\<nome motore>.log


Generale
Azioni
Aggiornamenti
Configura gli aggiornamenti automatici per questo profilo
Opzioni aggiornamento automatico
Configura le opzioni degli aggiornamenti automatici.
Controlla automaticamente aggiornamenti
Opzione download:
Controlla aggiornamenti e scarica
Intervallo di tempo di download:
1
ore
Ultimo aggiornamento:
07/05/2014 11:46:26
Opzioni di aggiornamento
Abilita le notifiche di posta per gli aggiornamenti completati
NOTA: le notifiche di aggiornamenti non riusciti verranno sempre inviate.
Per forzare il servizio di aggiornamento a effettuare il download degli aggiornamenti più recenti, fare clic sul pulsante sottostante.
Scarica aggiornamenti
Stato aggiornamento
Nessun aggiornamento in corso

Schermata 58: Schede Aggiornamenti motore

6. Per abilitare l'aggiornamento automatico per il del motore selezionato, dalla scheda **Aggiornamenti**, selezionare **Controlla automaticamente aggiornamenti**.

7. Dall'elenco **Opzione download**, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Controlla solo gli aggiornamenti	Selezionare questa opzione se si desidera che GFI MailEssentials controlli e notifichi solo l'amministratore quando sono disponibili aggiornamenti per il motore in questione. Questa opzione NON scaricherà automaticamente gli aggiornamenti disponibili.
Controlla aggiornamenti e scarica	Selezionare questa opzione se si desidera che GFI MailEssentials controlli e scarichi automaticamente eventuali aggiornamenti disponibili per il motore in questione.

8. Specificando un valore di intervallo in ore, indicare la frequenza con cui GFI MailEssentials deve controllare/scaricare gli aggiornamenti per questo motore.

9. Dall'area **Opzioni di aggiornamento**, selezionare **Abilita le notifiche di posta per gli aggiornamenti completati** per inviare una notifica di posta all'amministratore quando il motore si aggiorna correttamente.

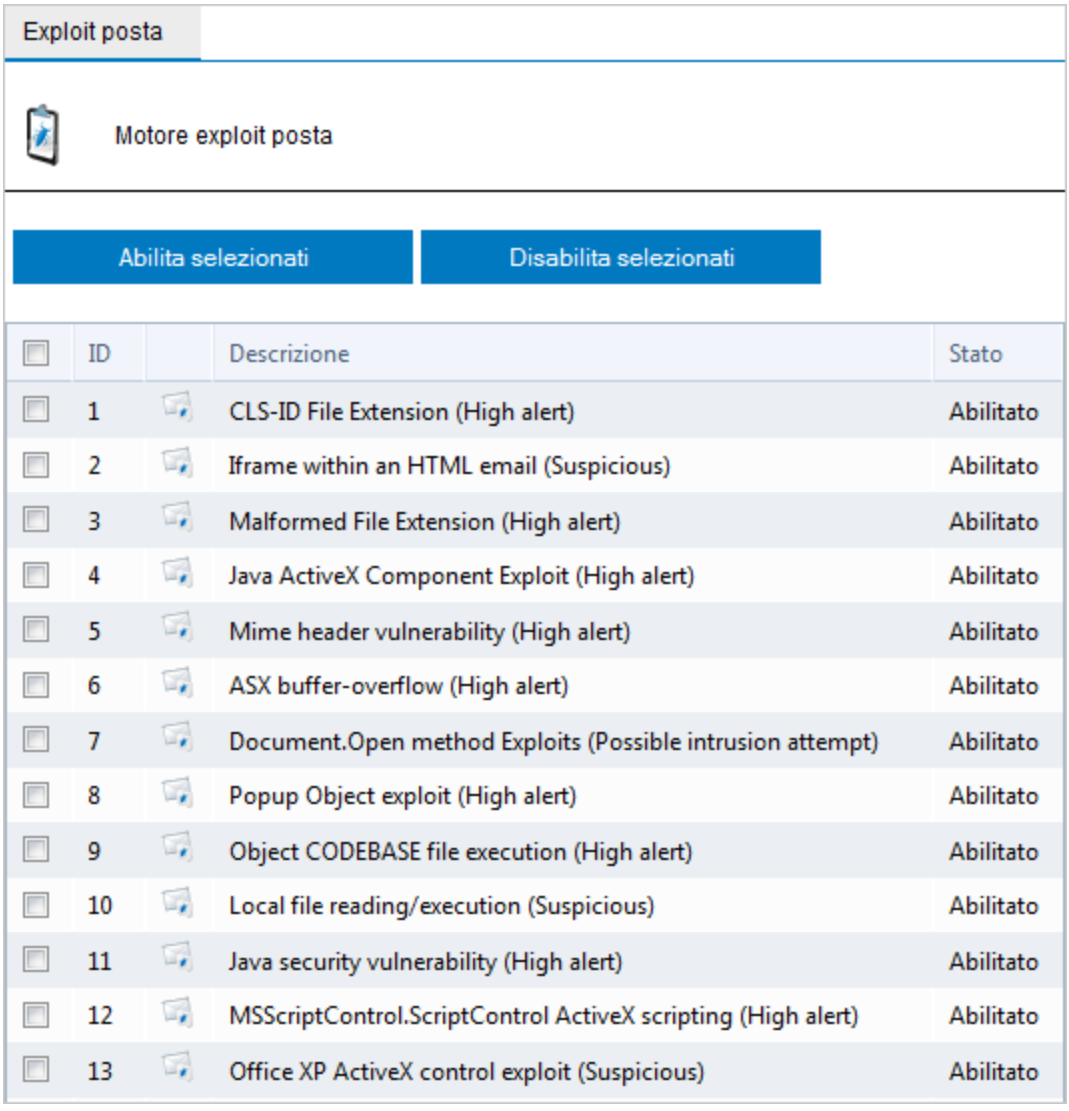
> **NOTA**
> Qualora l'aggiornamento non riuscisse, verrà sempre inviata una notifica di posta.

10. Per controllare e scaricare immediatamente gli aggiornamenti, fare clic su **Scarica aggiornamenti**.

11. Fare clic su **Applica**.

5.4.2 Abilitazione/disabilitazione exploit posta

1. Selezionare **Sicurezza e-mail > Motore exploit posta > Elenco exploit**.



ID	Descrizione	Stato
1	CLS-ID File Extension (High alert)	Abilitato
2	Iframe within an HTML email (Suspicious)	Abilitato
3	Malformed File Extension (High alert)	Abilitato
4	Java ActiveX Component Exploit (High alert)	Abilitato
5	Mime header vulnerability (High alert)	Abilitato
6	ASX buffer-overflow (High alert)	Abilitato
7	Document.Open method Exploits (Possible intrusion attempt)	Abilitato
8	Popup Object exploit (High alert)	Abilitato
9	Object CODEBASE file execution (High alert)	Abilitato
10	Local file reading/execution (Suspicious)	Abilitato
11	Java security vulnerability (High alert)	Abilitato
12	MSScriptControl.ScriptControl ActiveX scripting (High alert)	Abilitato
13	Office XP ActiveX control exploit (Suspicious)	Abilitato

Schermata 59: Elenco exploit posta

2. Selezionare la casella di controllo degli exploit per abilitarli o disabilitarli.

3. Di conseguenza, fare clic su **Abilita selezionati** o **Disabilita selezionati**.

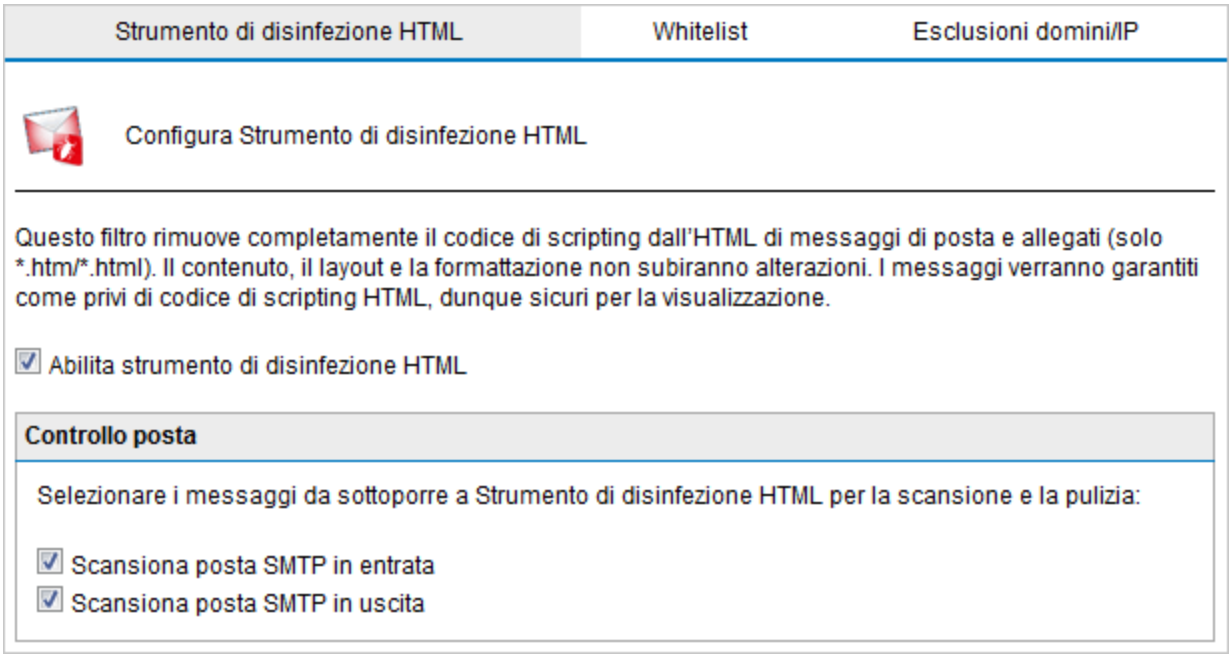
5.5 Strumento di disinfezione HTML

Strumento di disinfezione HTML scansiona e rimuove il codice di scripting presente nel corpo e negli allegati dei messaggi. Esegue la scansione di:

- corpo del messaggio dove il tipo MIME è impostato su “text/html”
- tutti gli allegati del tipo **.htm** o **.html**.

5.5.1 Configurazione strumento di disinfezione HTML

1. Selezionare **Sicurezza e-mail > Strumento di disinfezione HTML**.


Strumento di disinfezione HTML
Whitelist
Esclusioni domini/IP
Configura Strumento di disinfezione HTML
Questo filtro rimuove completamente il codice di scripting dall'HTML di messaggi di posta e allegati (solo *.htm/*.html). Il contenuto, il layout e la formattazione non subiranno alterazioni. I messaggi verranno garantiti come privi di codice di scripting HTML, dunque sicuri per la visualizzazione.
Abilita strumento di disinfezione HTML
Controllo posta
Selezionare i messaggi da sottoporre a Strumento di disinfezione HTML per la scansione e la pulizia:
Scansiona posta SMTP in entrata
Scansiona posta SMTP in uscita

Schermata 60: pagina di configurazione strumento di disinfezione HTML

2. Abilitare lo strumento di disinfezione HTML facendo clic sulla casella di controllo **Abilita strumento di disinfezione HTML**.

3. Selezionare la direzione dei messaggi:

Opzione	Descrizione
Scansiona posta SMTP in entrata	Scansiona e disinfetta gli script HTML di tutti i messaggi in entrata.
Scansiona posta SMTP in uscita	Scansiona e disinfetta gli script HTML di tutti i messaggi in uscita.

4. Fare clic su **Applica**.

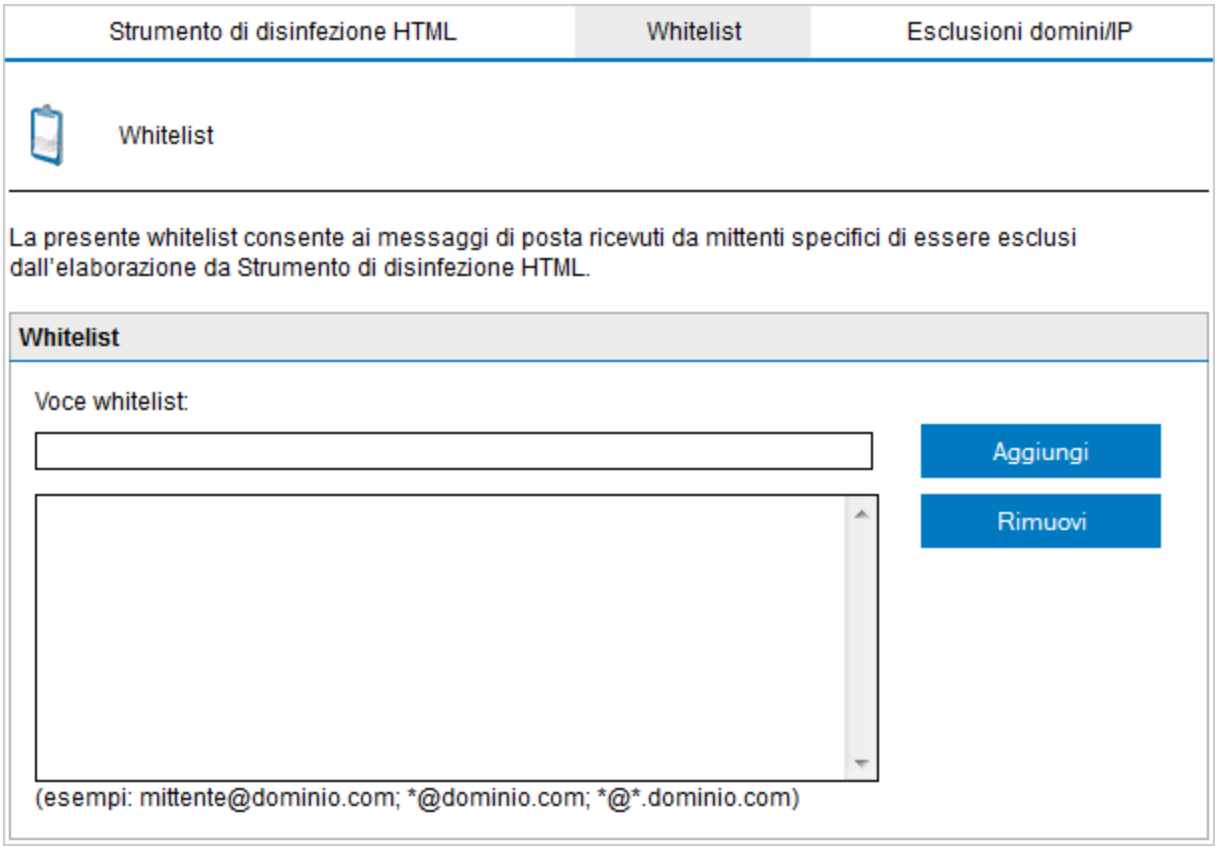
5.5.2 Whitelist strumento di disinfezione HTML

La whitelist dello strumento di disinfezione HTML può essere configurata per escludere i messaggi ricevuti da mittenti specifici.

NOTA
Per escludere indirizzi IP o domini specifici, utilizzare la funzione strumento di disinfezione HTML esclusioni dominio/IP. Per ulteriori informazioni, fare riferimento a Strumento di disinfezione HTML (pagina 105).

Per gestire i mittenti nella whitelist strumento di disinfezione HTML:

1. Selezionare **Sicurezza e-mail > Strumento di disinfezione HTML**, quindi fare clic sulla scheda **Whitelist**.



Schermata 61: pagina Whitelist strumento di disinfezione HTML

2. In **Voce whitelist**, digitare un indirizzo di posta, un dominio di posta (ad esempio, *@dominio.com) oppure un dominio secondario di posta (ad esempio, *@*.dominio.com), quindi fare clic su **Aggiungi**.

NOTA
Per rimuovere una voce dalla whitelist strumento di disinfezione HTML, selezionarla e fare clic su **Rimuovi**.

3. Fare clic su **Applica**.

5.5.3 Strumento di disinfezione HTML esclusioni dominio/ IP

La funzione Strumento di disinfezione HTML esclusioni dominio/IP consente agli amministratori di indicare gli indirizzi IP o i domini da escludere dallo Strumento di disinfezione HTML. Questo non utilizzerà semplicemente un elenco di indirizzi IP, può anche supportare gli indirizzi del dominio, che vengono anche risolti al runtime, così che sia possibile ottenere tutti gli indirizzi IP del dominio in questione. Esistono due modalità per eseguire questa operazione:

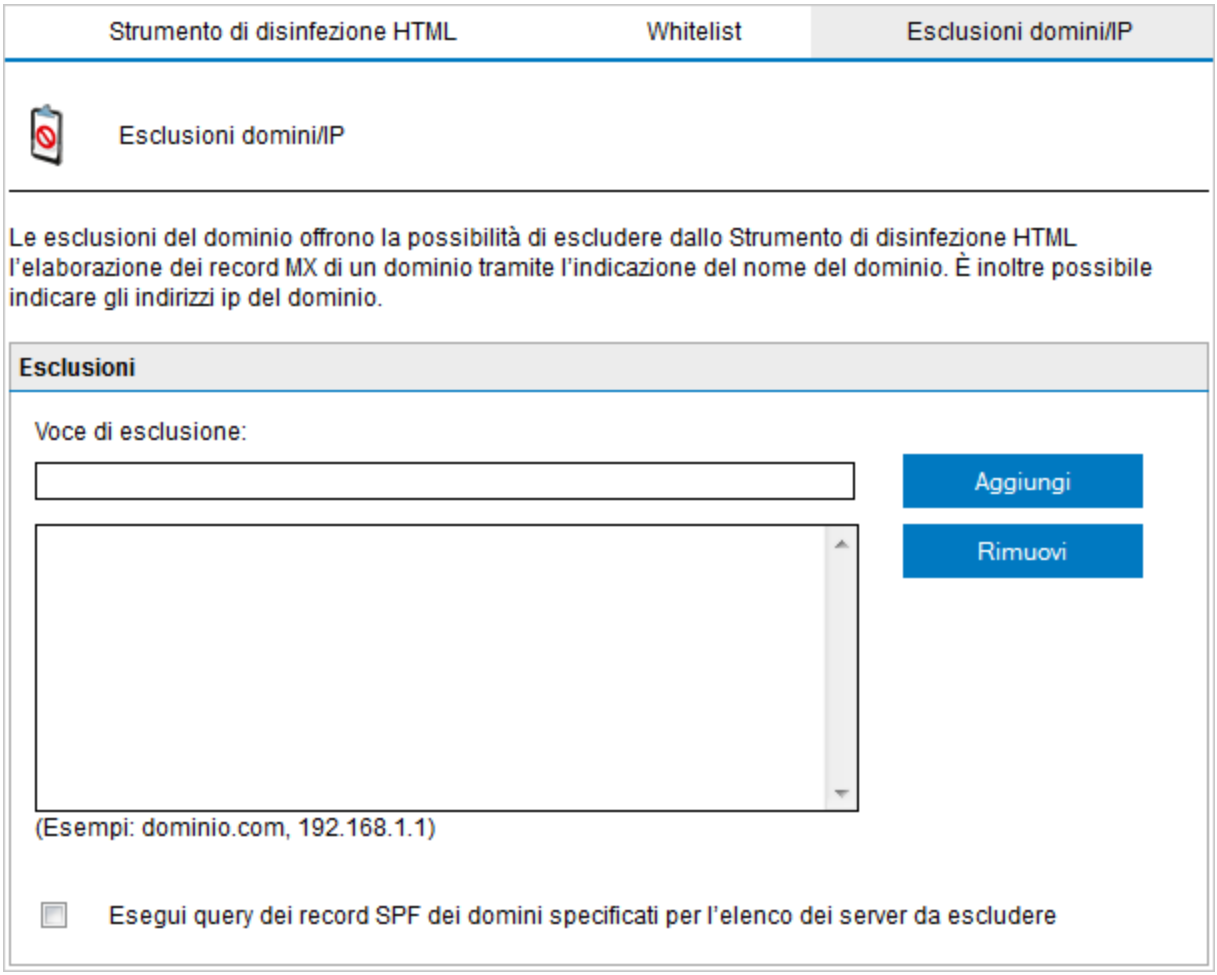
1. Per impostazione predefinita, la funzione esegue query sui record MX del dominio in fase di elaborazione.

2. In alternativa, è possibile scegliere di eseguire query al record SPF del dominio. Se il dominio non dispone di un record SPF, la parte SPF viene ignorata e si utilizzano solo i record MX.

Se l'indirizzo IP da cui parte il messaggio (quello inviato al server perimetrale) è un IP elencato nella scheda Esclusioni domini/IP oppure viene risolto da un dominio nel medesimo elenco, allora il messaggio non viene elaborato dallo Strumento di disinfezione HTML. È una sorta di whitelist IP ma con il vantaggio aggiuntivo di indicare i domini e di risolvere i record MX dei domini e (facoltativamente) il record SPF al fine di ottenere gli indirizzi IP.

Per gestire le esclusioni dei domini/IP nella whitelist dello strumento di disinfezione HTML:

1. Selezionare **Sicurezza e-mail > Strumento di disinfezione HTML**, quindi fare clic sulla scheda **Esclusioni domini/IP**.


Strumento di disinfezione HTML
Whitelist
Esclusioni domini/IP
Esclusioni domini/IP
Le esclusioni del dominio offrono la possibilità di escludere dallo Strumento di disinfezione HTML l'elaborazione dei record MX di un dominio tramite l'indicazione del nome del dominio. È inoltre possibile indicare gli indirizzi ip del dominio.
Esclusioni
Voce di esclusione:
Aggiungi
Rimuovi
(Esempi: dominio.com, 192.168.1.1)
Esegui query dei record SPF dei domini specificati per l'elenco dei server da escludere

Schermata 62: esclusioni domini/IP

2. Digitare un dominio o indirizzo IP da escludere e fare clic su **Aggiungi**.

> **NOTA**
> Per rimuovere una voce dalle Esclusioni dominio/IP dello strumento di disinfezione HTML, selezionarla e fare clic su **Rimuovi**.

3. In alternativa, selezionare **Esegui query dei record SPF dei domini specificati per l'elenco dei server da escludere**.

4. Fare clic su **Applica**.

6 Antispam

I filtri antispam inclusi in GFI MailEssentials aiutano a rilevare e bloccare i messaggi indesiderati (spam).

Argomenti del presente capitolo:

6.1 Filtri antispam 109
6.2 Operazioni antispam - cosa fare con lo spam. 148
6.3 Ordinamento filtri antispam in base alla priorità. 151
6.4 Filtraggio trasmissione SMTP 152
6.5 Spam Digest 154
6.6 Impostazioni antispam 156
6.7 SpamTag per Microsoft Outlook 162
6.8 Scansione cartella pubblica 170

6.1 Filtri antispam

GFI MailEssentials utilizza vari filtri di scansione per identificare lo spam:

FILTRO	DESCRIZIONE	ABILITATO PER IMPOSTAZIONE PREDEFINITA
SpamRazer	Un motore antispam che riconosce se un messaggio di posta elettronica è spam attraverso impronte digitali, reputazione e analisi del contenuto dei messaggi.	Sì
Antiphishing	Blocca i messaggi che contengono collegamenti ai corpi del messaggio che indirizzano a siti noti di phishing o che contengono parole chiave di phishing tipiche.	Sì
Raccolta di directory	Gli attacchi di Raccolta di directory si verificano quando gli spammer cercano di indovinare gli indirizzi di posta allegando i nomi utente noti al dominio della vittima. La maggioranza degli indirizzi di posta elettronica è inesistente.	Sì (solo se GFI MailEssentials è installato in un ambiente Active Directory)
Block list e-mail	La Block list e-mail è un database personalizzato di indirizzi di posta elettronica e domini da cui non si desidera ricevere alcun messaggio.	Sì
Block list IP	La Block list IP è un database personalizzato di indirizzi IP da cui non si desidera ricevere alcun messaggio.	No
Block list DNS IP	Block list DNS IP controlla l'indirizzo IP del server di invio della posta con un elenco pubblico di server di posta noti per l'invio di spam.	Sì
Block list DNS URI	Arresta i messaggi che contengono collegamenti a domini elencati nelle block list URI spam.	Sì
Sender Policy Framework	Questo filtro utilizza i record SPF per arrestare i messaggi inviati da indirizzi IP falsificati, identificando se l'indirizzo IP del mittente è autorizzato.	No
Anti-spoofing	I messaggi ricevuti con un indirizzo e-mail del mittente e che sembrano provenire dal proprio dominio vengono controllati da GFI MailEssentialssulla base di un elenco di indirizzi IP. Se l'indirizzo IP del mittente non è presente nell'elenco di indirizzi IP del server del proprio dominio, il messaggio verrà bloccato.	No

FILTRO	DESCRIZIONE	ABILITATO PER IMPOSTAZIONE PREDEFINITA
Greylist	Il filtro greylist blocca temporaneamente i messaggi di posta in arrivo ricevuti da mittenti sconosciuti. Normalmente, i sistemi di posta attendibili ritentano l'invio dopo alcuni minuti, gli spammer invece ignorano tali messaggi di errore.	No
Rilevamento lingua	Determina la lingua del testo del corpo del messaggio ed è configurabile per il blocco di determinate lingue.	No
Controllo intestazione	Il filtro Controllo intestazione analizza l'intestazione e-mail per identificare i messaggi spam.	No
Controllo parole chiave spam	Questo filtro consente l'identificazione dello spam sulla base di parole chiave all'interno del messaggio ricevuto.	No
Analisi bayesiana	Un filtro antispam che può essere addestrato per determinare con precisione se un messaggio è spam in base a quanto rilevato in precedenza.	No
Whitelist	La whitelist contiene gli elenchi dei criteri che identificano la posta attendibile. Le e-mail che rispettano tali criteri non saranno scansionate dai filtri antispam e verranno sempre recapitate al destinatario.	Sì
Nuovi mittenti	Il filtro Nuovi mittenti identifica i messaggi di posta elettronica inviati da mittenti ai quali non sono mai stati inviati messaggi.	No

6.1.1 SpamRazer

Un motore antispam che riconosce se un messaggio di posta elettronica è spam attraverso impronte digitali, reputazione e analisi del contenuto dei messaggi. SpamRazer è il motore antispam principale ed è abilitato per impostazione predefinita al momento dell'installazione. Vengono rilasciati aggiornamenti frequenti per SpamRazer, che ridurranno ulteriormente i tempi di risposta alle nuove tendenze spam.

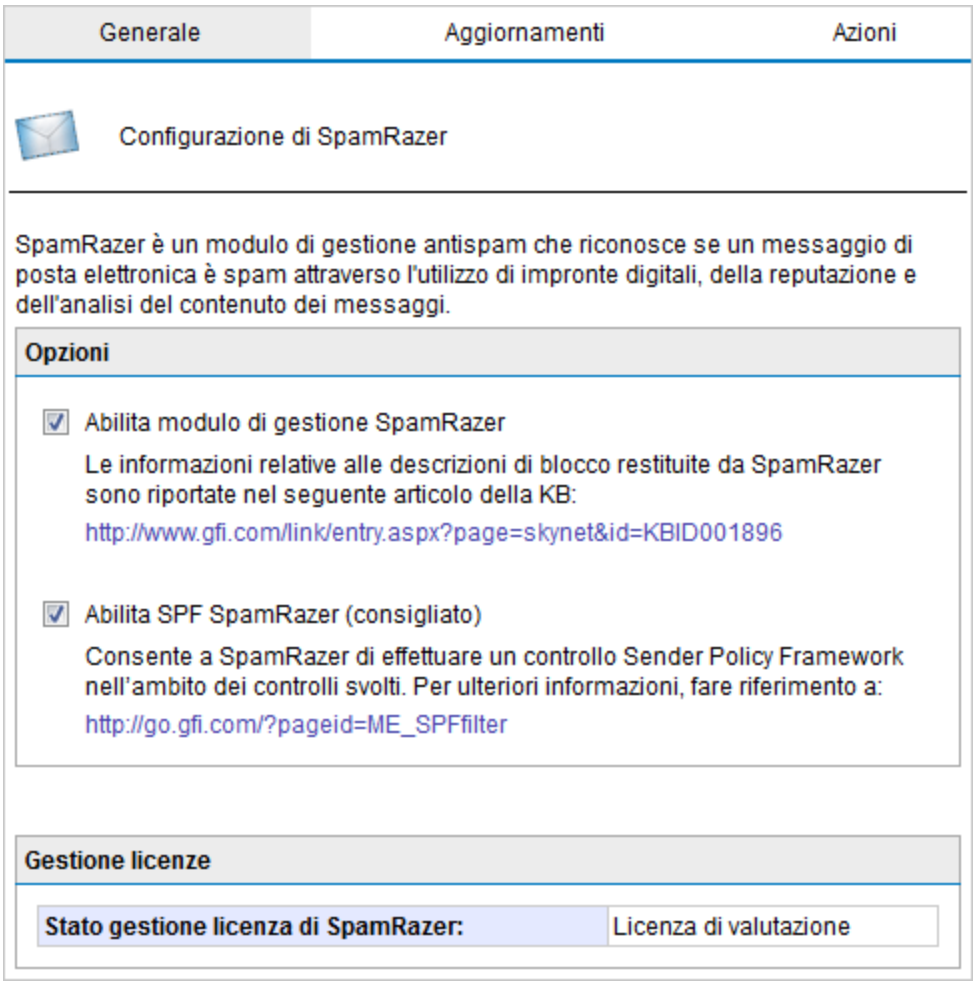
SpamRazer include anche il filtro Sender Policy Framework che rileva i mittenti manomessi. È consigliabile che i mittenti pubblichino il proprio server di posta in un record SPF. Per maggiori informazioni su SPF e sul relativo funzionamento, visitare il sito web di Sender Policy Framework all'indirizzo: http://www.openspf.org.

Questo filtro blocca anche lo spam NDR. Per ulteriori informazioni sullo spam NDR, fare riferimento a http://go.gfi.com/?pageid=ME_NDRSpam

Configurazione di SpamRazer

> **NOTE**
>
> 1. La disabilitazione di SpamRazer **NON** è consigliata.
> 2. GFI MailEssentials scarica gli aggiornamenti di SpamRazer da: ***.mailshell.net**

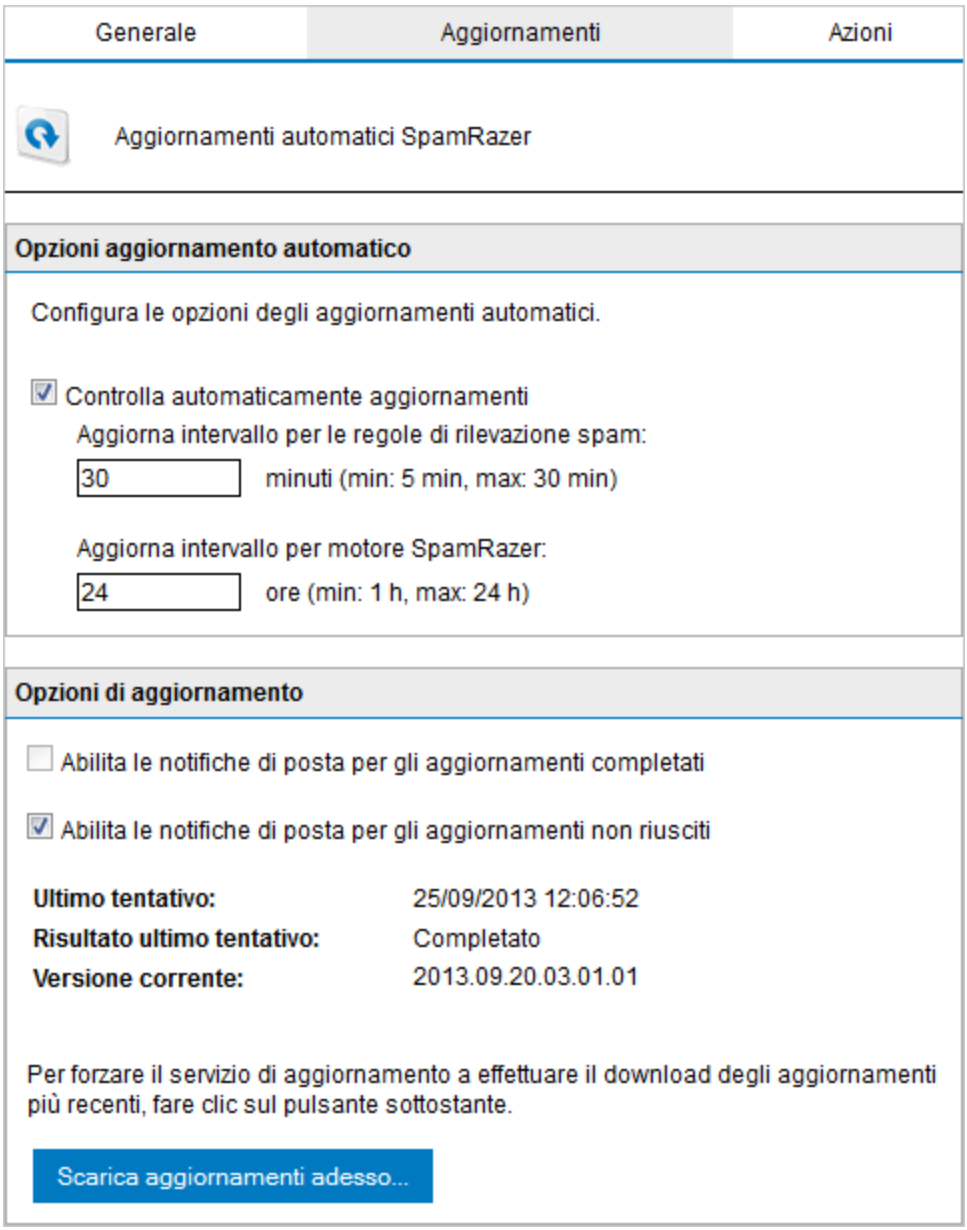
1. Selezionare **Antispam > Filtri antispam > SpamRazer**.


Generale
Aggiornamenti
Azioni
Configurazione di SpamRazer
SpamRazer è un modulo di gestione antispam che riconosce se un messaggio di posta elettronica è spam attraverso l'utilizzo di impronte digitali, della reputazione e dell'analisi del contenuto dei messaggi.
Opzioni
Abilita modulo di gestione SpamRazer
Le informazioni relative alle descrizioni di blocco restituite da SpamRazer sono riportate nel seguente articolo della KB:
http://www.gfi.com/link/entry.aspx?page=skynet&id=KBID001896
Abilita SPF SpamRazer (consigliato)
Consente a SpamRazer di effettuare un controllo Sender Policy Framework nell'ambito dei controlli svolti. Per ulteriori informazioni, fare riferimento a:
http://go.gfi.com/?pageid=ME_SPFfilter
Gestione licenze
Stato gestione licenza di SpamRazer:
Licenza di valutazione

Schermata 63: proprietà SpamRazer

2. Dalla scheda **Generale**, effettuare una delle seguenti operazioni:

Opzione	Descrizione
Abilita modulo di gestione SpamRazer	Abilitare o disabilitare SpamRazer.
Abilita SPF SpamRazer (consigliato)	Abilitare o disabilitare Sender Policy Framework. Si consiglia di abilitare questa opzione e di eseguire il filtro dopo whitelist e-mail.


Generale
Aggiornamenti
Azioni
Aggiornamenti automatici SpamRazer
Opzioni aggiornamento automatico
Configura le opzioni degli aggiornamenti automatici.
Controlla automaticamente aggiornamenti
Aggiorna intervallo per le regole di rilevazione spam:
30
minuti (min: 5 min, max: 30 min)
Aggiorna intervallo per motore SpamRazer:
24
ore (min: 1 h, max: 24 h)
Opzioni di aggiornamento
Abilita le notifiche di posta per gli aggiornamenti completati
Abilita le notifiche di posta per gli aggiornamenti non riusciti
Ultimo tentativo:
25/09/2013 12:06:52
Risultato ultimo tentativo:
Completato
Versione corrente:
2013.09.20.03.01.01
Per forzare il servizio di aggiornamento a effettuare il download degli aggiornamenti più recenti, fare clic sul pulsante sottostante.
Scarica aggiornamenti adesso...

Schermata 64: scheda aggiornamenti SpamRazer

3. Dalla scheda **Aggiornamenti**, effettuare una delle seguenti operazioni:

Opzione	Descrizione
Controlla automaticamente aggiornamenti	Configurare GFI MailEssentials affinché controlli e scarichi in automatico gli aggiornamenti di SpamRazer. Specifica un intervallo di tempo in minuti al termine del quale dovrà essere eseguito il controllo della regola di rilevazione spam e degli aggiornamenti del motore SpamRazer. **NOTA** Si consiglia di abilitare questa opzione affinché SpamRazer sia più efficace nel rilevare le ultime tendenze di spam.
Abilita le notifiche di posta per gli aggiornamenti completati	Selezionare questa opzione per essere informati via posta elettronica quando sono scaricati nuovi aggiornamenti.

Opzione	Descrizione
Abilita le notifiche di posta per gli aggiornamenti non riusciti	Selezionare questa opzione per essere informati via posta elettronica quando un download o un'installazione fallisce.
Scarica aggiornamenti adesso...	Fare clic per scaricare gli aggiornamenti.

> **NOTA**
> Gli aggiornamenti possono essere scaricati utilizzando un server proxy. Per ulteriori informazioni, fare riferimento a Impostazioni proxy (pagina 242).

4. Per selezionare le azioni da effettuare sui messaggi identificati come spam, fare clic sulla scheda **Azioni**. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148).

5. Fare clic su **Applica**.

6.1.2 Antiphishing

Blocca i messaggi che contengono collegamenti ai corpi del messaggio che indirizzano a siti noti di phishing o che contengono parole chiave di phishing tipiche. Il phishing è una tecnica di ingegneria sociale basata sulla posta il cui scopo è portare gli utenti della posta a rivelare i propri dati personali agli spammer. Un messaggio di phishing è molto probabilmente realizzato in modo da assomigliare a un messaggio originale proveniente da un'azienda rinomata, ad esempio una banca. Normalmente i messaggi di phishing contengono istruzioni che richiedono la riconferma di informazioni di natura sensibile da parte degli utenti, come i dati bancari o le informazioni sulla carta di credito. Di solito, i messaggi di phishing includono un URI (Uniform Resource Identifier) che l'utente deve seguire per inserire alcune informazioni di natura sensibile su un sito di phishing. Il sito indicato dall'URI di phishing potrebbe essere una replica di un sito ufficiale ma in realtà è controllato dalla persona che ha inviato i messaggi di phishing. Quando l'utente immette le informazioni sensibili nel sito di phishing, i dati vengono raccolti e utilizzati, ad esempio, per ritirare denaro dai conti bancari.

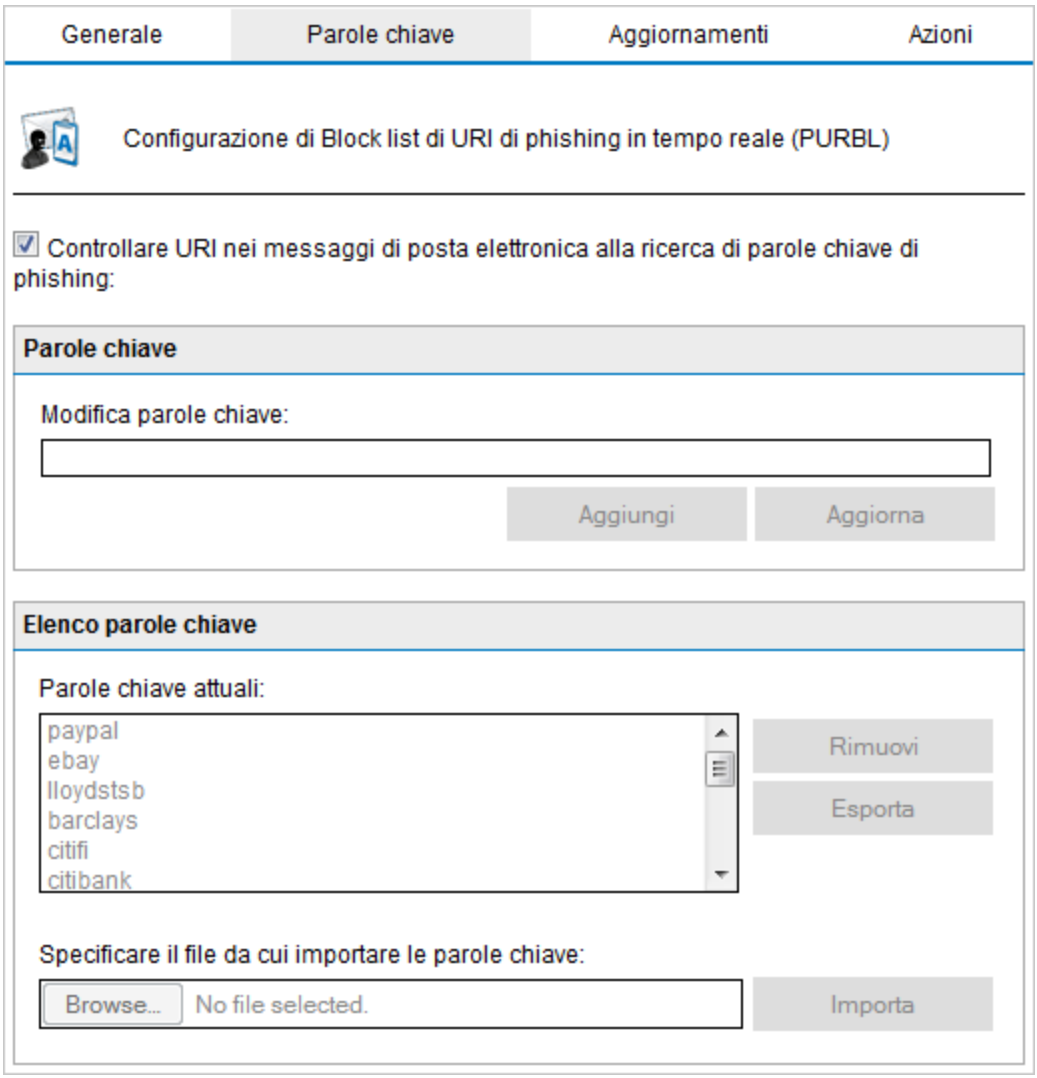
Il filtro antiphishing rileva i messaggi di phishing confrontando gli URI presenti nel messaggio con un database di URI noti per essere utilizzati negli attacchi di phishing. Il phishing cerca negli URI anche le parole chiave tipiche utilizzate nel phishing.

Il filtro antiphishing è abilitato per impostazione predefinita al momento dell'installazione.

Configurazione antiphishing

> **NOTA**
> **NON** si consiglia di disabilitare l'antiphishing.

1. Selezionare **Antispam > Filtri antispam > Antiphishing**.



Schermata 65: opzioni antiphishing

2. Per abilitare/disabilitare l'antiphishing, nella scheda **Generale**, selezionare/deselezionare l'opzione **Controllare i messaggi di posta elettronica alla ricerca di URI di siti di phishing conosciuti.**

3. Nella scheda **Parole chiave**, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Controllare URI nei messaggi di posta elettronica alla ricerca di parole chiave tipiche di phishing.	Abilita/disabilita controlli per le parole chiave tipiche di phishing
Aggiungi	Consente l'aggiunta di parole chiave al filtro antiphishing. Digitare la parola chiave e fare clic su **Aggiungi** per aggiungerla al filtro antiphishing.
Aggiorna	Consente l'aggiornamento di parole chiave selezionate. Selezionare una parola chiave dall'elenco **Parole chiave attuali**, eseguire le dovute modifiche alla parola chiave dal campo **Modifica parole chiave** e quindi fare clic su **Aggiorna**.
Rimuovi	Consente la rimozione delle parole chiave selezionate dall'elenco. Selezionare una parola chiave dall'elenco **Parole chiave attuali**, quindi fare clic su **Rimuovi**.

Opzione	Descrizione
Esporta	Esporta l'elenco attuale in un file di formato XML.
Sfoglia...	Consente l'importazione di un elenco parole chiave precedentemente esportato. Fare clic su **Sfoglia**, selezionare un file di parole chiave precedentemente esportato e quindi fare clic su **Importa**.

4. Dalla scheda **Aggiornamenti**, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Controlla automaticamente aggiornamenti	Configurare GFI MailEssentials affinché controlli e scarichi in automatico gli aggiornamenti di antiphishing. Specifica un intervallo di tempo in minuti al termine del quale dovrà essere eseguito il controllo degli aggiornamenti. **NOTA** Si consiglia di abilitare questa opzione affinché l'antiphishing sia più efficace nel rilevare le ultime tendenze di phishing.
Abilita le notifiche di posta per gli aggiornamenti completati	Selezionare/deselezionare la casella di controllo per essere informati via posta elettronica quando sono scaricati nuovi aggiornamenti.
Abilita le notifiche di posta per gli aggiornamenti non riusciti	Selezionare/selezionare questa casella per essere informati quando un download o un installazione non viene eseguita.
Scarica aggiornamenti adesso...	Fare clic su questa opzione per scaricare immediatamente gli aggiornamenti antiphishing.

NOTA

Gli aggiornamenti possono essere scaricati utilizzando un server proxy. Per ulteriori informazioni, fare riferimento a Impostazioni proxy (pagina 242).

5. Per selezionare le azioni da effettuare sui messaggi identificati come spam, fare clic sulla scheda **Azioni**. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148).

6. Fare clic su **Applica**.

6.1.3 Raccolta di directory

Gli attacchi di Raccolta di directory si verificano quando gli spammer cercano di indovinare gli indirizzi di posta allegando i nomi utente noti al dominio della vittima. La maggioranza degli indirizzi di posta elettronica è inesistente. Gli spammer inviano i messaggi di posta a indirizzi di posta elettronica generati in modo casuale. Anche se alcuni indirizzi possono corrispondere a utenti reali, la gran parte di questi messaggi non è valida e dunque inonda il server di posta della vittima.

GFI MailEssentials arresta questi attacchi bloccando i messaggi di posta indirizzati a utenti che non fanno parte di Active Directory o del server di posta dell'organizzazione.

La raccolta di directory può essere configurata per essere eseguita al ricevimento del messaggio completo o a livello SMTP, dunque i messaggi vengono filtrati mentre vengono ricevuti. Il filtro a livello SMTP interrompe la connessione della posta e dunque arresta il download dell'intero messaggio, risparmiando la larghezza di banda e le risorse di elaborazione. In questo caso, la

connessione viene interrotta immediatamente e i messaggi non devono superare nessun altro filtro antispam.

Questo filtro è abilitato per impostazione predefinita al momento dell'installazione di GFI MailEssentials in un ambiente Active Directory.

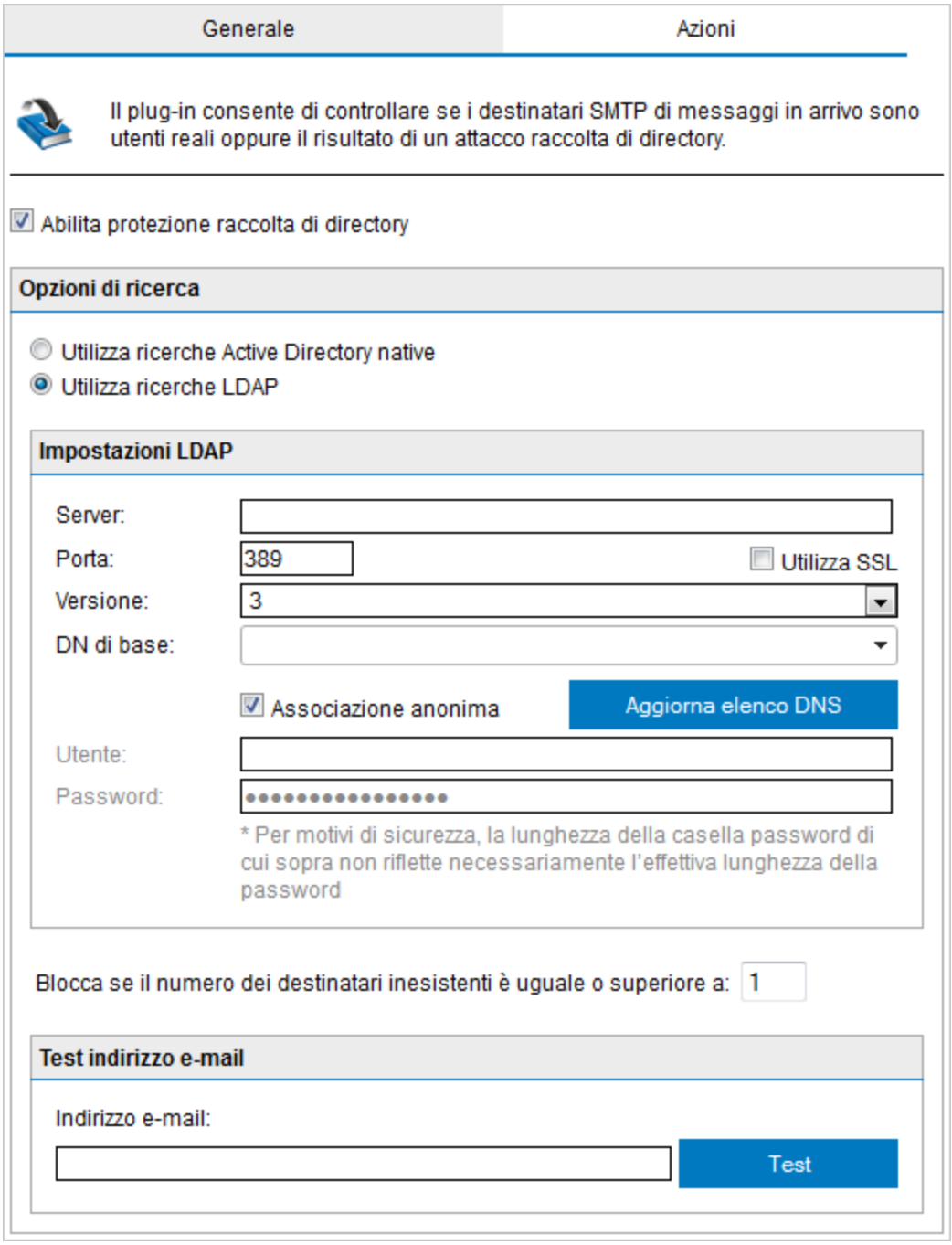
La raccolta di directory si configura in due passaggi, nel modo seguente:

Fase 1 - Configurazione proprietà Raccolta di directory

Fase 2 - Scegliere se eseguire Raccolta di directory durante la trasmissione SMTP.

Fase 1 - Configurazione proprietà Raccolta di directory

1. Selezionare **Antispam > Filtri antispam > Raccolta di directory**.


Generale
Azioni
Il plug-in consente di controllare se i destinatari SMTP di messaggi in arrivo sono utenti reali oppure il risultato di un attacco raccolta di directory.
Abilita protezione raccolta di directory
Opzioni di ricerca
Utilizza ricerche Active Directory native
Utilizza ricerche LDAP
Impostazioni LDAP
Server:
Porta:
389
Utilizza SSL
Versione:
3
DN di base:
Associazione anonima
Aggiorna elenco DNS
Utente:
Password:
* Per motivi di sicurezza, la lunghezza della casella password di cui sopra non riflette necessariamente l'effettiva lunghezza della password
Blocca se il numero dei destinatari inesistenti è uguale o superiore a:
1
Test indirizzo e-mail
Indirizzo e-mail:
Test

Schermata 66: pagina Raccolta di directory

2. Abilitare/disabilitare Raccolta di directory e selezionare il metodo di ricerca da utilizzare:

Opzione	Descrizione
Abilita protezione raccolta di directory	Abilitare/disabilitare Raccolta di directory.
Utilizza ricerche Active Directory native	Scegliere questa opzione se GFI MailEssentials è installato in Active Directory. **NOTA** Quando GFI MailEssentials si trova dietro un firewall, la funzione di Raccolta di directory potrebbe non essere in grado di connettersi direttamente alla Active Directory interna a causa delle impostazioni del firewall. Utilizzare le ricerche LDAP per eseguire la connessione all'Active Directory interna della rete e assicurarsi di abilitare la porta predefinita 389/636 sul firewall.
Utilizza ricerche LDAP	Selezionare la configurazione delle impostazioni LDAP se GFI MailEssentials è installato nella modalità SMTP. Se il server LDAP richiede autenticazione, deselezionare l'opzione **Associazione anonima** e immettere i dati di autenticazione che verranno utilizzati da questa funzione. **NOTA** Specificare le credenziali di autenticazione utilizzando il formato Dominio/Utente (ad esempio dominio-principale\amministratore). **NOTA** In un'Active Directory, il server LDAP è solitamente il controller di dominio.

3. Nell'opzione **Blocca se il numero dei destinatari inesistenti è uguale o superiore a**, indicare il numero di destinatari inesistenti che porterà alla classificazione del messaggio come spam. Se i destinatari di un messaggio non sono validi o se il numero di destinatari non validi è uguale o superiore al limite specificato, i messaggi verranno bloccati tramite raccolta di directory.

> **NOTA**
> Evitare i falsi positivi impostando un numero ragionevole nella casella di modifica **Blocca se il numero dei destinatari inesistenti è uguale o superiore a**. Il valore deve tenere conto degli utenti che inviano posta attendibile a indirizzi e-mail digitati erroneamente oppure a utenti che non sono più impiegati presso l'azienda. È consigliabile impostare questo valore almeno su **2**.

4. Fornire un indirizzo di posta e fare clic su **Test** per verificare le impostazioni di Raccolta di directory. Ripetere il test con un indirizzo di posta elettronica inesistente e assicurarsi che la ricerca Active Directory non abbia esito positivo.

5. Per selezionare le azioni da effettuare sui messaggi identificati come spam, fare clic sulla scheda **Azioni**. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148).

> **NOTA**
> Se Raccolta di directory è impostata per essere eseguita a livello SMTP, solo l'opzione **Registra occorrenza regola nel seguente file** sarà disponibile nella scheda **Azioni**.

6. Fare clic su **Applica**.

Fase 2 - Scegliere se eseguire Raccolta di directory durante la trasmissione SMTP.

1. Accedere a **Antispam > Priorità filtro** e selezionare la scheda **Filtraggio trasmissione SMTP**.

2. Fare clic su **Cambia** per attivare o disattivare il filtro di Raccolta di directory scegliendo tra:

Opzione	Descrizione
Filtraggio alla ricezione dei messaggi di posta completi	Il filtraggio viene effettuato alla ricezione dell'intero messaggio.
Filtraggio durante trasmissione SMTP	Il filtraggio viene effettuato durante la trasmissione SMTP attraverso la verifica dell'esistenza dei destinatari del messaggio, prima della ricezione del corpo del messaggio e dell'allegato. **NOTA** Se viene selezionata questa opzione, Raccolta di directory verrà sempre eseguita prima degli altri filtri antispam.

3. Fare clic su **Applica**.

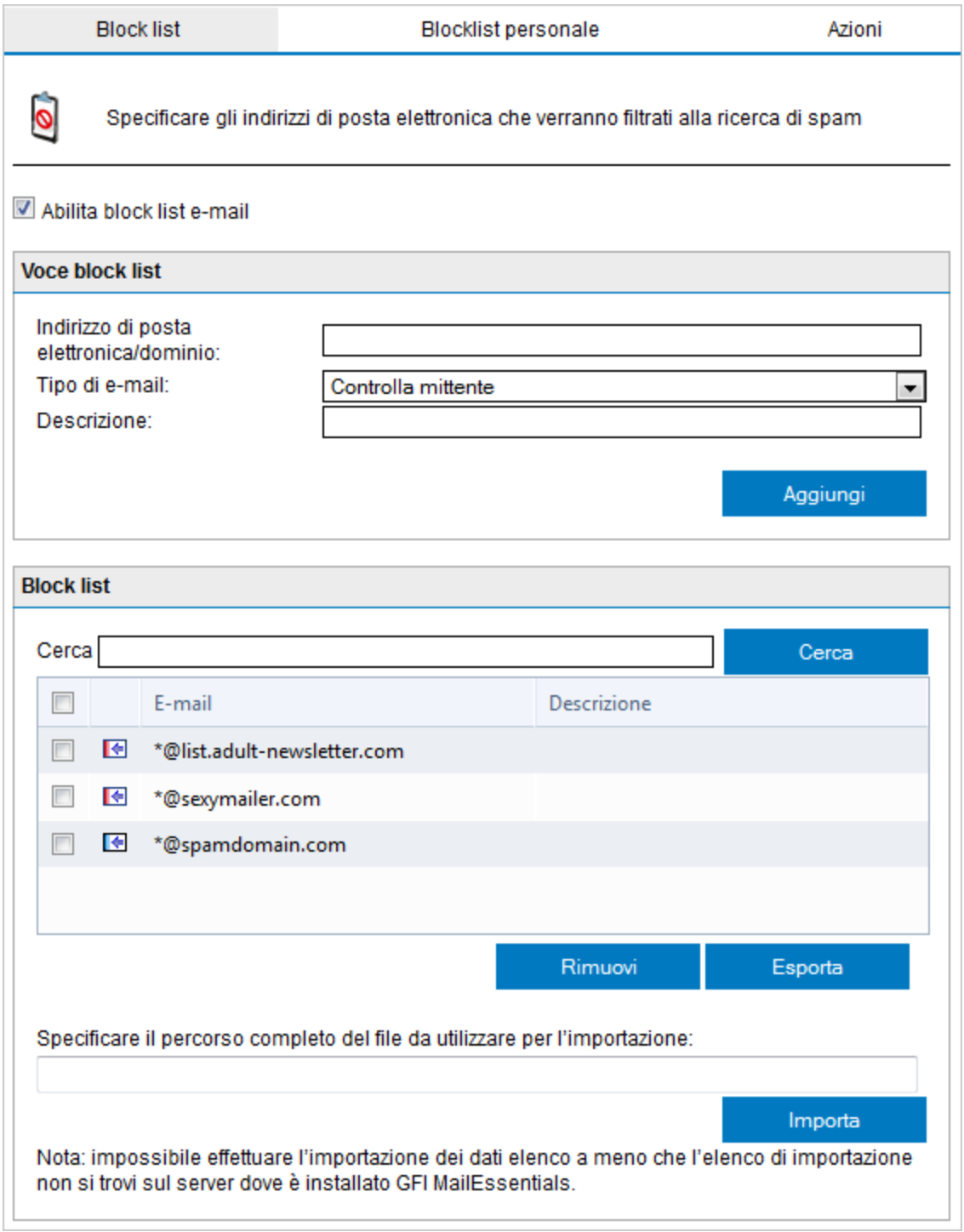
6.1.4 Block list e-mail

La Block list e-mail è un database personalizzato di indirizzi di posta elettronica e domini da cui non si desidera ricevere alcun messaggio.

Questo filtro è abilitato per impostazione predefinita al momento dell'installazione di GFI MailEssentials.

Configurazione di Block list e-mail

1. Accedere a **Antispam > Filtri antispam > Block list e-mail**.



Schermata 67: Block list e-mail

2. Dalla scheda **Block list**, configurare gli indirizzi e-mail e i domini da bloccare.

OPZIONE	DESCRIZIONE
Abilita block list e-mail	Selezionare/deselezionare per abilitare/disabilitare la block list e-mail.

OPZIONE	DESCRIZIONE
Aggiungi	Aggiungere alla block list indirizzi e-mail, domini di posta elettronica o un suffisso dell'intero dominio. 1. Digitare l'indirizzo e-mail, il dominio (ad esempio, *@spammer.com) o un suffisso dell'intero dominio (ad esempio *@*.tv) da aggiungere alla block list. 2. Indicare il tipo di messaggio a cui devono corrispondere i messaggi da inserire nella whitelist. **NOTA** Per ulteriori informazioni sulla differenza tra SMTP e MIME fare riferimento a: http://go.gfi.com/?pageid=ME_DifferenceSMTPMIME 3. (Facoltativo) È anche possibile aggiungere una descrizione alla voce nel campo Descrizione. 4. Fare clic su **Aggiungi**.
Rimuovi	Selezionare una voce della block list e fare clic su **Rimuovi** per eliminarla.
Importa	Importa un elenco di voci di block list da un file in formato XML. **NOTA** È possibile importare un elenco di voci da un file in formato XML con la medesima struttura utilizzata da GFI MailEssentials per l'esportazione di un elenco di voci.
Esporta	Esporta l'elenco di voci della block list in un file in formato XML.
Cerca	Digitare una voce da cercare. Le voci corrispondenti vengono filtrate nell'elenco di voci della block list.

3. Per selezionare le azioni da effettuare sui messaggi identificati come spam, fare clic sulla scheda **Azioni**. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148).

4. Fare clic su **Applica**.

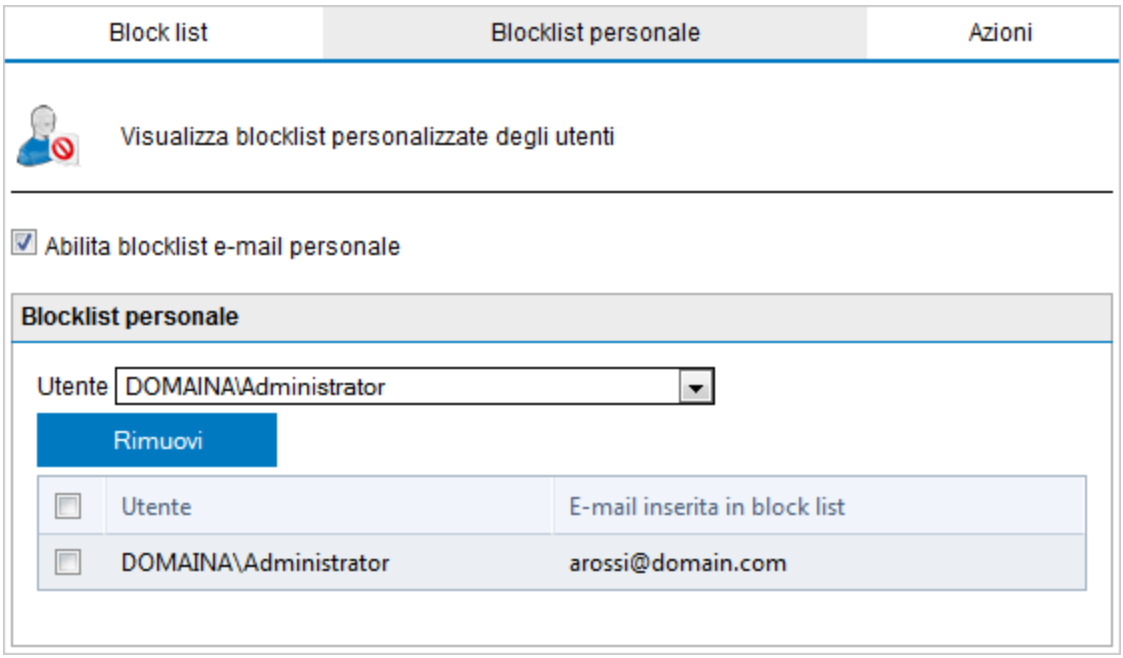
Blocklist personale

La block list personale è una block list aggiuntiva che completa la block list globale. Disabilitata per impostazione predefinita, la blocklist personale può essere abilitata per gli utenti per consentir loro di aggiungere indirizzi di posta specifici a una blocklist personale che possano gestire. Per ulteriori informazioni, fare riferimento a Azioni utente finale (pagina 21).

Per gli scopi di gestione, gli amministratori possono anche rimuovere indirizzi di posta specifici che gli utenti hanno aggiunto alla loro blocklist personale.

Abilitazione/disabilitazione blocklist personale

1. Selezionare **Antispam > Block list e-mail**.



Schermata 68: blocklist personale

2. Selezionare la scheda **Blocklist personale** e selezionare o deselezionare **Abilita blocklist e-mail personale** per abilitare o disabilitare la funzione della blocklist personale.

3. Fare clic su **Applica**.

Rimozione dei messaggi dalla blocklist personale degli utenti

1. Accedere a **Antispam > Block list e-mail** e selezionare la scheda **Blocklist personale**.

2. Dall'elenco a discesa **Utente**, selezionare l'utente di cui eliminare un indirizzo di posta.

3. Selezionare un indirizzo di posta dall'elenco. Fare clic su **Rimuovi**.

4. Fare clic su **Applica**.

6.1.5 Block list IP

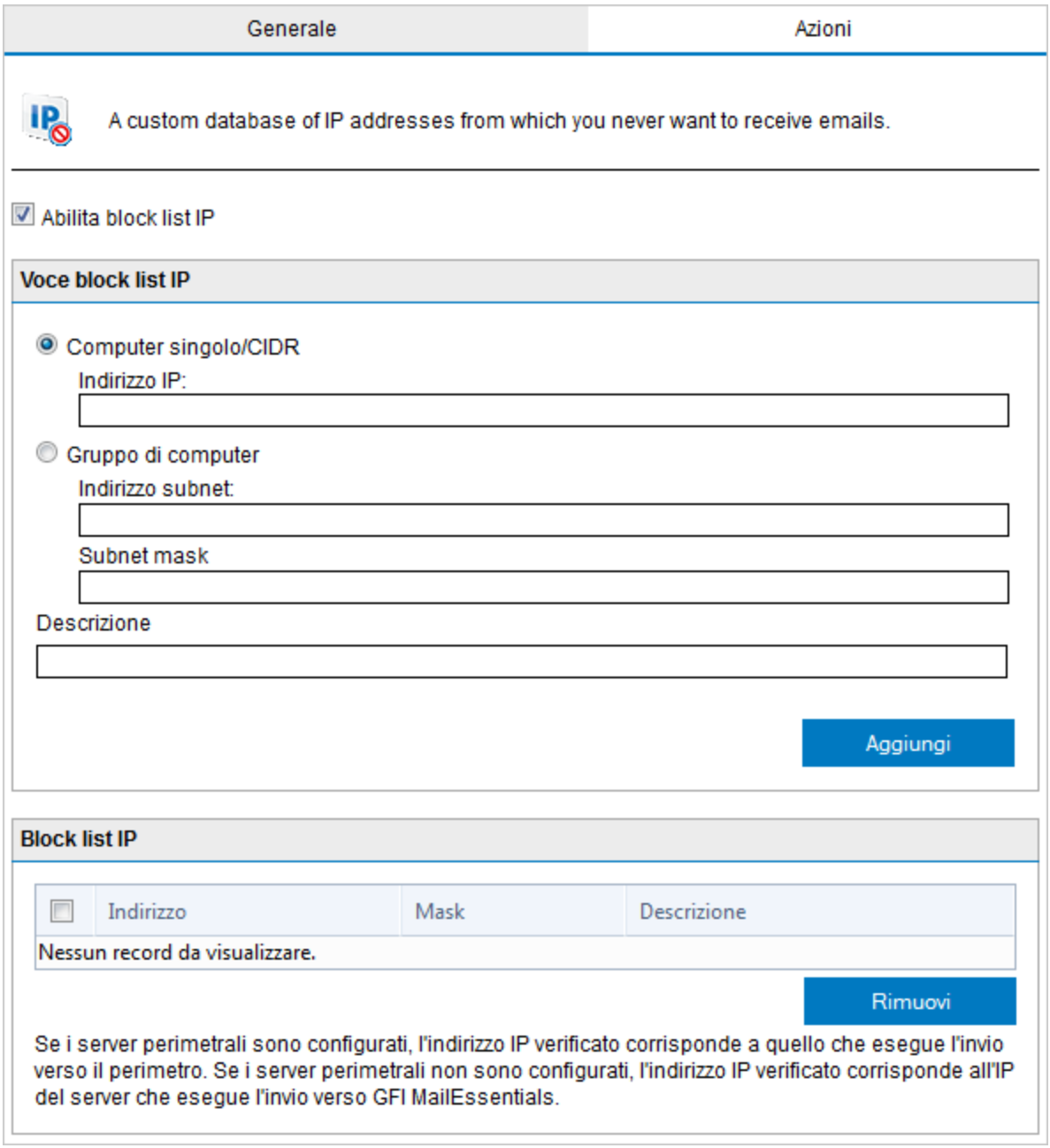
La Block list IP è un database personalizzato di indirizzi IP da cui non si desidera ricevere alcun messaggio.

Questo filtro può essere configurato per essere eseguito al ricevimento del messaggio completo o a livello SMTP, dunque i messaggi vengono filtrati mentre vengono ricevuti. Il filtro a livello SMTP interrompe la connessione della posta e dunque arresta il download dell'intero messaggio, risparmiando la larghezza di banda e le risorse di elaborazione. In questo caso, la connessione viene interrotta immediatamente e i messaggi non devono superare nessun altro filtro antispam. Per ulteriori informazioni, fare riferimento a Filtraggio trasmissione SMTP (pagina 152).

La block list IP NON è abilitata per impostazione predefinita.

Configurazione whitelist

1. Accedere a **Antispam > Filtri antispam > Block list IP**.


Generale
Azioni
A custom database of IP addresses from which you never want to receive emails.
Abilita block list IP
Voce block list IP
Computer singolo/CIDR
Indirizzo IP:
Gruppo di computer
Indirizzo subnet:
Subnet mask
Descrizione
Aggiungi
Block list IP
Indirizzo
Mask
Descrizione
Nessun record da visualizzare.
Rimuovi
Se i server perimetrali sono configurati, l'indirizzo IP verificato corrisponde a quello che esegue l'invio verso il perimetro. Se i server perimetrali non sono configurati, l'indirizzo IP verificato corrisponde all'IP del server che esegue l'invio verso GFI MailEssentials.

Schermata 69: Block list IP

2. Dalla scheda **Generale**, selezionare **Abilita block list IP** per bloccare tutti i messaggi di posta elettronica ricevuti da indirizzi IP specifici.

3. Nella casella **Voce block list IP**, specificare gli indirizzi IP da bloccare:

Opzione	Descrizione
Computer singolo/CIDR	Immettere un singolo indirizzo IP o un intervallo di indirizzi IP utilizzando la notazione CIDR.
Gruppo di computer	Indicare **Indirizzo subnet** e **Subnet Mask** del gruppo di IP da inserire in whitelist. 2. (Facoltativo) Aggiungere una **Descrizione**. 3 Fare clic su **Aggiungi**.
Descrizione	Se lo si desidera, è possibile aggiungere una descrizione per facilitare l'identificazione degli IP specificati.

4. Fare clic su **Aggiungi** per aggiungere gli indirizzi IP specificati alla casella **Block list IP**.

5. Per eliminare gli indirizzi IP dalla Block list IP, selezionare gli indirizzi da rimuovere e fare clic su **Rimuovi**.

6. Per selezionare le azioni da effettuare sui messaggi identificati come spam, fare clic sulla scheda **Azioni**. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148).

> **NOTA**
> Se Block list IP è impostata per essere eseguita a livello SMTP, solo l'opzione **Registra occorrenza regola nel seguente file** sarà disponibile nella scheda **Azioni**.

7. Fare clic su **Applica**.

6.1.6 Block list DNS IP

Block list DNS IP controlla l'indirizzo IP del server di invio della posta con un elenco pubblico di server di posta noti per l'invio di spam. GFI MailEssentials supporta una serie di block list DNS IP. Esiste una serie di Block list DNS IP disponibili, che partono da elenchi affidabili con procedure chiaramente delineate per l'inserimento o la rimozione dalle stesse fino a elenchi meno affidabili.

GFI MailEssentials mantiene una cache con i risultati delle query alla block list DNS IP onde evitare che vengano eseguite query multiple alle block list DNS IP per i medesimi indirizzi IP. Gli elementi rimangono nella cache per 4 giorni e vengono cancellati al riavvio del servizio GFI MailEssentials AS Scan Engine.

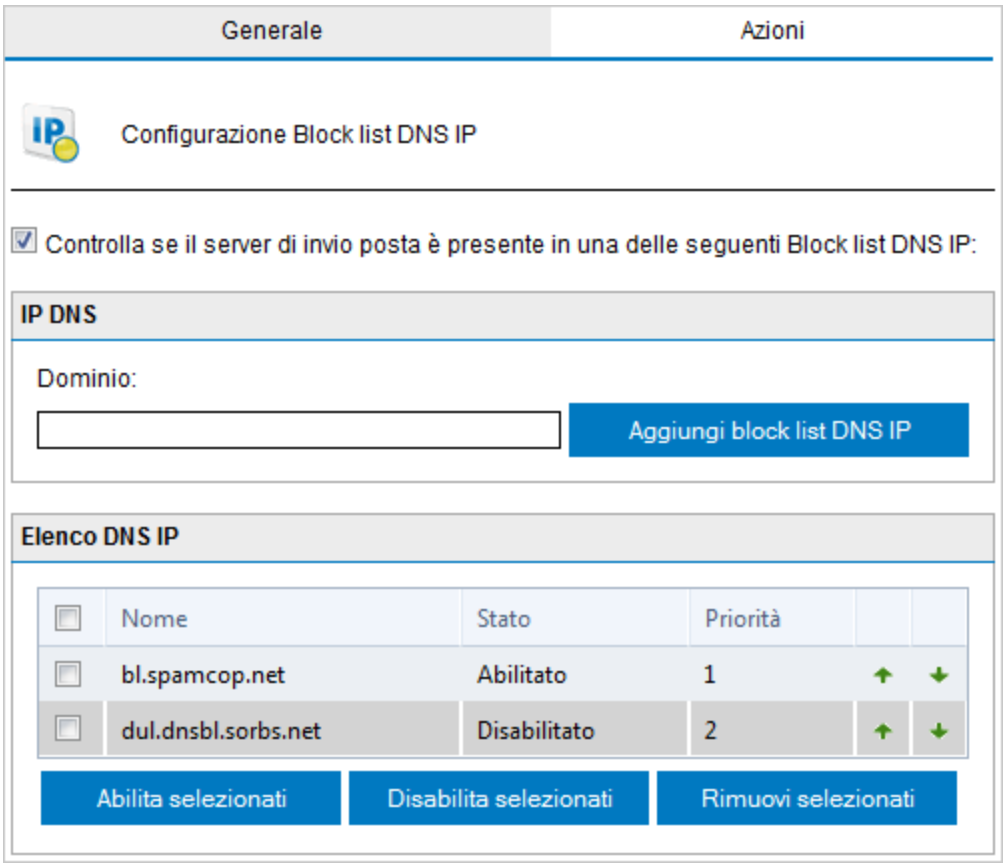
Questo filtro può essere configurato per essere eseguito al ricevimento del messaggio completo o a livello SMTP, dunque i messaggi vengono filtrati mentre vengono ricevuti. Il filtro a livello SMTP interrompe la connessione della posta e dunque arresta il download dell'intero messaggio, risparmiando la larghezza di banda e le risorse di elaborazione. In questo caso, la connessione viene interrotta immediatamente e i messaggi non devono superare nessun altro filtro antispam. Per ulteriori informazioni, fare riferimento a Filtraggio trasmissione SMTP (pagina 152).

Questo filtro è abilitato per impostazione predefinita al momento dell'installazione di GFI MailEssentials.

> **Note importanti**
>
> 1. Affinché questa funzione sia disponibile, il server DNS deve essere configurato correttamente. In caso contrario, si verificheranno timeout e il traffico della posta verrà rallentato. Per maggiori informazioni, consultare: http://go.gfi.com/?pageid=ME_ProcessingSlow
>
> 2. L'invio di query a una block list DNS IP può risultare lento, a seconda della connessione, dunque la posta può subire leggeri rallentamenti.
>
> 3. Assicurarsi che tutti i server perimetrali SMTP siano configurati nella finestra di dialogo Server perimetrali SMTP, così da consentire a GFI MailEssentials di controllare l'indirizzo IP che si connette ai server perimetrali. Per ulteriori informazioni, fare riferimento a Impostazioni server SMTP perimetrali (pagina 239).

Configurazione block list DNS IP

1. Accedere a **Antispam > Filtri antispam > Block list DNS IP**.



Schermata 70: Block list DNS IP

2. Configurare le opzioni seguenti:

Opzione	Descrizione
Controlla se il server di invio posta è presente in una delle seguenti Block list DNS IP:	Selezionare questa opzione per abilitare il filtro block list DNS IP.
Aggiungi block list DNS IP	Se necessario, aggiungere altre block list DNS IP a quelle già elencate. Immettere il dominio della block list DNS IP e fare clic su **Aggiungi block list DNS IP**.
Abilita selezionati	Selezionare una block list DNS IP e fare clic su **Abilita selezionati** per abilitarla.
Disabilita selezionati	Selezionare una block list di IP DNS e fare clic su **Disabilita selezionati** per disabilitarla.
Rimuovi selezionati	Selezionare una block list DNS IP e fare clic su **Rimuovi selezionati** per rimuoverla.

3. Per selezionare le azioni da effettuare sui messaggi identificati come spam, fare clic sulla scheda **Azioni**. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148).

4. Fare clic su **Applica**.

NOTA

Per abilitare la block list DNS IP a livello di filtro trasmissione SMTP, selezionare la scheda **Antispam > Priorità filtro > Filtraggio trasmissione SMTP** e fare clic su **Parametro** accanto alla blocklist DNS IP per abilitare/disabilitare il filtro a livello SMTP oppure alla ricezione del messaggio completo.

6.1.7 Block list DNS URI

Arresta i messaggi che contengono collegamenti a domini elencati nelle block list URI spam.

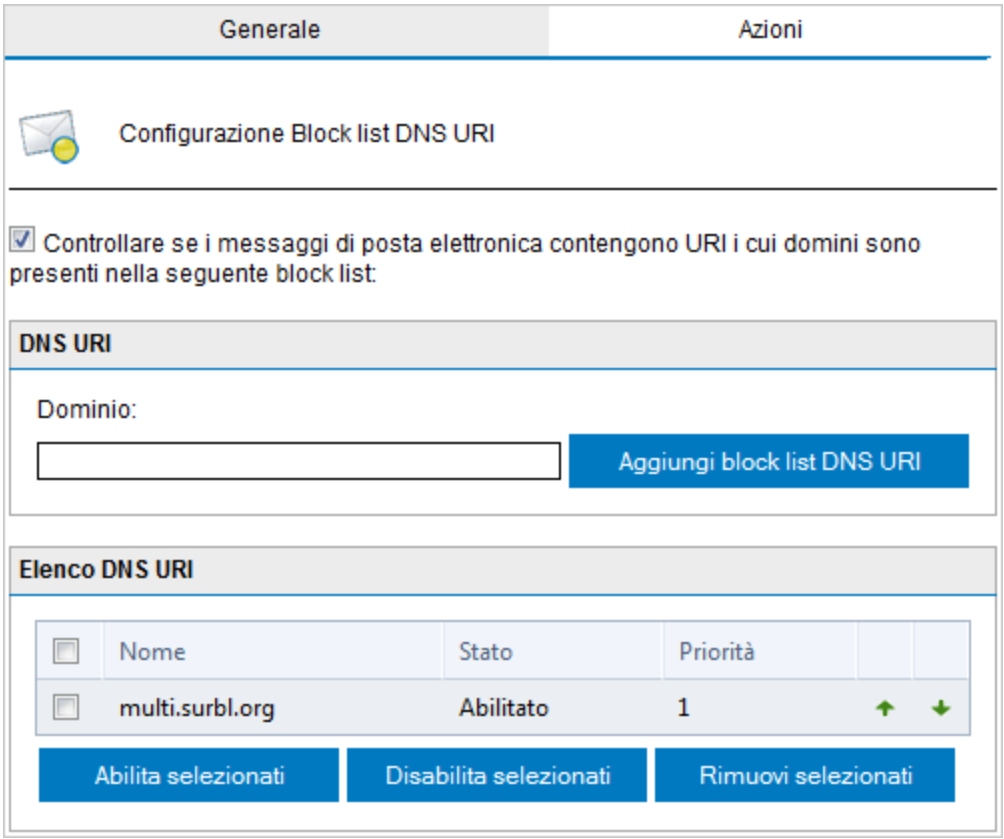
Un URI (Universal Resource Identifier) è uno strumento standard per indirizzare le risorse sul web.

Le RBL (Realtime Blocklist) rilevano lo spam sulla base di collegamenti ipertestuali nella posta che sono noti essere utilizzati dagli spammer.

Questo filtro è abilitato per impostazione predefinita al momento dell'installazione di GFI MailEssentials.

Configurazione block list DNS URI

1. Selezionare **Antispam > Filtri antispam > Block list DNS URI**.



Schermata 71: Block list DNS URI

2. Dalla scheda **Block list DNS URI**:

Opzione	Descrizione
Controllare se i messaggi di posta elettronica contengono URI i cui domini sono presenti nelle seguenti block list:	Per abilitare il filtro block list DNS URI, selezionare questa opzione.
Aggiungi block list DNS URI	Se necessario, aggiungere altre block list DNS URI a quelle già elencate. Immettere il nome completo del dominio della block list DNS URI e fare clic su **Aggiungi block list DNS URI**.
Ordine di preferenza	L'ordine di preferenza per le block list abilitare DNS URI può essere cambiato selezionando una block list e facendo clic sui pulsanti Su o Giù.
Abilita selezionati	Selezionare una block list DNS URI e fare clic su **Abilita selezionati** per attivarla. **NOTA** Si consiglia di disabilitare tutte le altre block list DNS URI al momento di abilitare **multi.surbl.org**, in quanto ciò potrebbe incrementare il tempo di elaborazione dei messaggi.
Disabilita selezionati	Selezionare una block list DNS URI e fare clic su **Disabilita selezionati** per disattivarla.
Rimuovi selezionati	Selezionare una block list DNS URI e fare clic su **Rimuovi selezionati** per rimuoverla.

3. Per selezionare le azioni da effettuare sui messaggi identificati come spam, fare clic sulla scheda **Azioni**. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148).

4. Fare clic su **Applica**.

6.1.8 Sender Policy Framework

Questo filtro utilizza i record SPF per arrestare i messaggi inviati da indirizzi IP falsificati, identificando se l'indirizzo IP del mittente è autorizzato. Il filtro Sender Policy Framework è basato su un impegno della community, il che richiede che i mittenti pubblichino gli indirizzi IP dei loro server di posta in un record SPF.

Esempio: Se un messaggio viene inviato da xyz@CompanyABC.com, allora companyABC.com deve pubblicare un record SPF per poter determinare se il messaggio è stato davvero inviato dalla rete companyABC.com oppure è un falso. Se un record SPF non viene pubblicato da CompanyABC.com, il risultato SPF sarà 'sconosciuto'.

Per ulteriori informazioni su SPF e sul funzionamento, visitare il sito web di Sender Policy Framework all'indirizzo:

http://www.openspf.org.

Il filtro SPF NON è abilitato per impostazione predefinita e si consiglia di abilitare questa opzione e di anteporne l'esecuzione rispetto alla Whitelist e-mail, in modo da bloccare i mittenti falsificati prima che siano erroneamente inseriti nella whitelist.

La pubblicazione dei record SPF da parte di GFI MailEssentials non è un requisito del programma. Per pubblicare i record SPF, utilizzare la procedura guidata SPF presente in:

http://www.openspf.org/wizard.html.

Prerequisiti

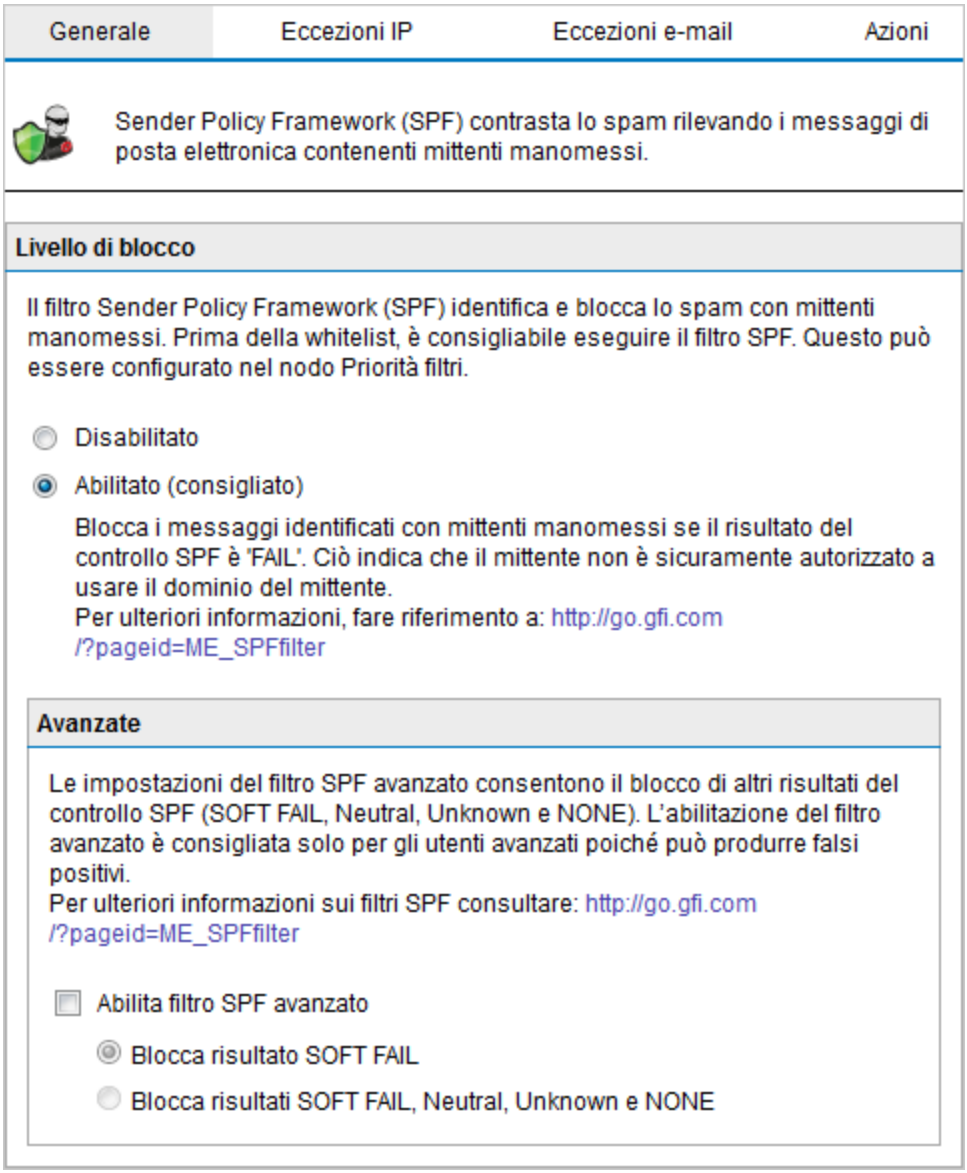
Prima di abilitare il filtro Sender Policy Framework su un'installazione server non-gateway:

1. Andare a **Impostazioni generali > Server SMTP perimetrali**.

2. Nell'opzione di impostazione del server perimetrale SMTP, fare clic su **Rileva** per effettuare una ricerca MX DNS e definire in automatico l'indirizzo IP del server SMTP perimetrale.

Abilitazione di Sender Policy Framework

1. Selezionare **Antispam > Filtri antispam > Sender Policy Framework**.


Generale
Eccezioni IP
Eccezioni e-mail
Azioni
Sender Policy Framework (SPF) contrasta lo spam rilevando i messaggi di posta elettronica contenenti mittenti manomessi.
Livello di blocco
Il filtro Sender Policy Framework (SPF) identifica e blocca lo spam con mittenti manomessi. Prima della whitelist, è consigliabile eseguire il filtro SPF. Questo può essere configurato nel nodo Priorità filtri.
Disabilitato
Abilitato (consigliato)
Blocca i messaggi identificati con mittenti manomessi se il risultato del controllo SPF è 'FAIL'. Ciò indica che il mittente non è sicuramente autorizzato a usare il dominio del mittente.
Per ulteriori informazioni, fare riferimento a: http://go.gfi.com/?pageid=ME_SPFfilter
Avanzate
Le impostazioni del filtro SPF avanzato consentono il blocco di altri risultati del controllo SPF (SOFT FAIL, Neutral, Unknown e NONE). L'abilitazione del filtro avanzato è consigliata solo per gli utenti avanzati poiché può produrre falsi positivi.
Per ulteriori informazioni sui filtri SPF consultare: http://go.gfi.com/?pageid=ME_SPFfilter
Abilita filtro SPF avanzato
Blocca risultato SOFT FAIL
Blocca risultati SOFT FAIL, Neutral, Unknown e NONE

Schermata 72: abilitazione e configurazione delle proprietà Sender Policy Framework (SPF)

2. Per abilitare Sender Policy Framework, fare clic su **Abilitato**. Se l'indirizzo IP del mittente del messaggio non è assolutamente autorizzato a inviare i messaggi dal dominio del mittente, i messaggi di posta saranno bloccati.

3. In alternativa, selezionare **Abilita filtro SPF avanzato** e selezionare una delle opzioni avanzate da:

OPZIONE	DESCRIZIONE
Blocca risultato SOFT FAIL	Blocca tutti i messaggi dove: » L'indirizzo IP del mittente non è assolutamente autorizzato a inviare messaggi dal dominio del mittente » L'indirizzo IP del mittente probabilmente non è autorizzato a inviare messaggi dal dominio del mittente. Per ulteriori informazioni sui filtri SPF avanzati, consultare: http://go.gfi.com/?pageid=ME_SPFfilter
Blocca risultati SOFT FAIL, Neutral, Unknown e NONE	Blocca tutti i messaggi dove: » L'indirizzo IP del mittente non è assolutamente autorizzato a inviare messaggi dal dominio del mittente » L'indirizzo IP del mittente probabilmente non è autorizzato a inviare messaggi dal dominio del mittente » L'indirizzo IP del mittente è decisamente non convincente, sconosciuto o non esistono dati pubblicati in merito. Per ulteriori informazioni sui filtri SPF avanzati, consultare: http://go.gfi.com/?pageid=ME_SPFfilter

4. Selezionare la scheda **Eccezioni IP** o **Eccezioni e-mail** per configurare gli indirizzi IP e/o i destinatari da escludere dai controlli SPF:

» **Elenco eccezioni IP:** Le voci del presente elenco superano in automatico i controlli SPF. Selezionare la casella di controllo **Elenco eccezioni IP**, aggiungere un nuovo indirizzo IP e descrizione, quindi fare clic su **Aggiungi**. Per rimuovere le voci, selezionare quelle da rimuovere dall'elenco e fare clic su **Rimuovi selezionati**. Per disabilitare l'elenco eccezioni IP, deselezionare la casella di controllo **Elenco eccezioni IP**.

> **NOTA**
> Quando si aggiungono manualmente gli indirizzi IP all'elenco eccezioni IP, è anche possibile aggiungere un intervallo di indirizzi IP tramite la notazione CIDR.

» **Elenco eccezioni messaggi:** Questa opzione assicura che determinati mittenti o destinatari dei messaggi siano esclusi dal controllo SPF, anche se i messaggi vengono respinti. Selezionare la casella di controllo **Elenco eccezioni messaggi**, aggiungere un nuovo indirizzo di posta elettronica e descrizione, quindi fare clic su **Aggiungi**. Per rimuovere le voci, selezionare quelle da rimuovere dall'elenco e fare clic su **Rimuovi selezionati**. Per disabilitare l'elenco eccezioni messaggi, deselezionare la casella di controllo **Elenco eccezioni messaggi**. Un indirizzo e-mail può essere immesso in uno dei seguenti tre modi:

- local part - 'abuse' (corrisponde a 'abuse@abc.com', 'abuse@xyz.com', ecc...)
- domain - '@abc.com' (corrisponde a 'john@abc.com', 'jill@abc.com', ecc...)
- complete - 'joe@abc.com' (corrisponde solo a 'joe@abc.com')

5. Per selezionare le azioni da effettuare sui messaggi identificati come spam, fare clic sulla scheda **Azioni**. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148).

6. Fare clic su **Applica** per salvare le impostazioni.

6.1.9 Anti-spoofing

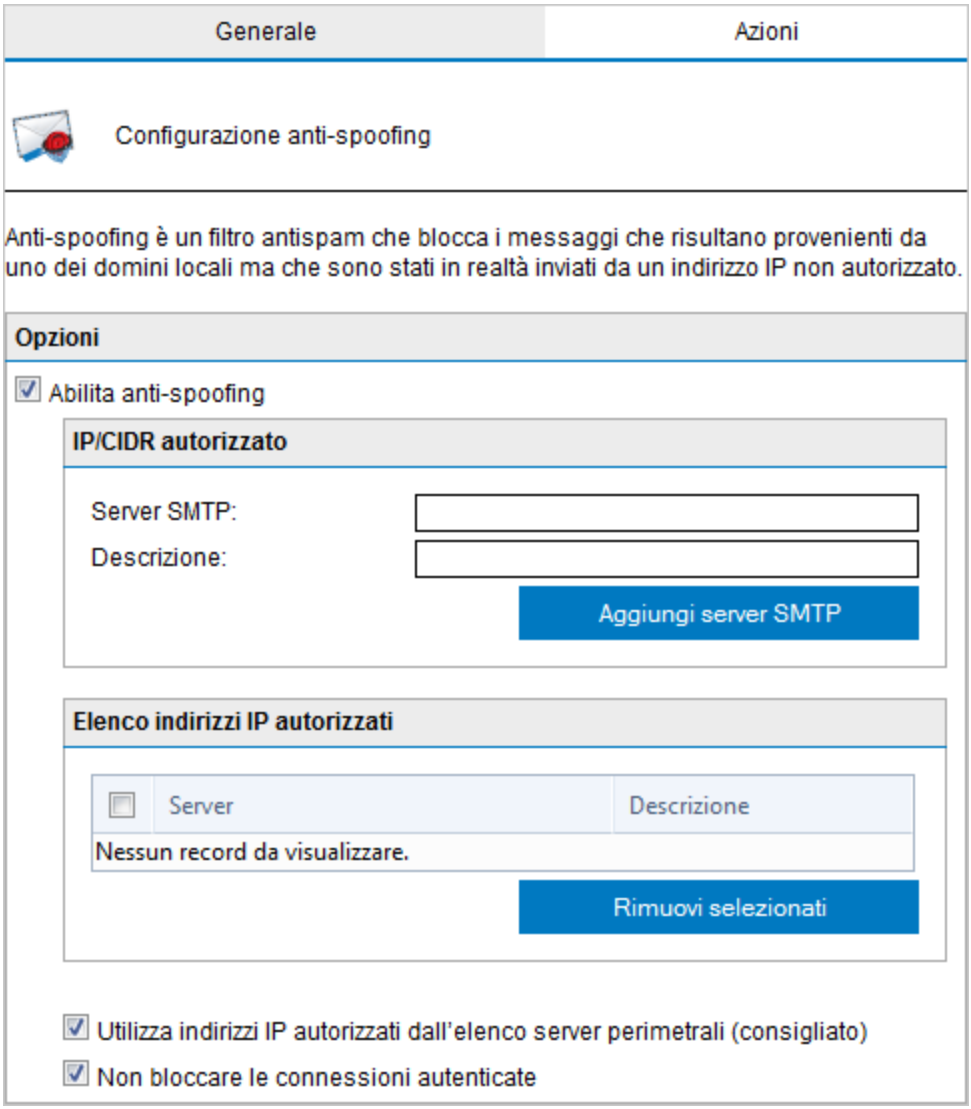
I messaggi ricevuti con un indirizzo e-mail del mittente e che sembrano provenire dal proprio dominio vengono controllati da GFI MailEssentialssulla base di un elenco di indirizzi IP. Se l'indirizzo IP del mittente non è presente nell'elenco di indirizzi IP del server del proprio dominio, il messaggio verrà bloccato.

Questo filtro NON è abilitato per impostazione predefinita.

> **AVVISO**
> Se si abilita questa funzione, non inserire nella whitelist gli utenti interni, poiché rende vano il controllo anti-spoofing.

Abilitazione e configurazione anti-spoofing

1. Selezionare **Antispam > Filtri antispam > Anti-spoofing**.


Generale
Azioni
Configurazione anti-spoofing
Anti-spoofing è un filtro antispam che blocca i messaggi che risultano provenienti da uno dei domini locali ma che sono stati in realtà inviati da un indirizzo IP non autorizzato.
Opzioni
Abilita anti-spoofing
IP/CIDR autorizzato
Server SMTP:
Descrizione:
Aggiungi server SMTP
Elenco indirizzi IP autorizzati
Server
Descrizione
Nessun record da visualizzare.
Rimuovi selezionati
Utilizza indirizzi IP autorizzati dall'elenco server perimetrali (consigliato)
Non bloccare le connessioni autenticate

Schermata 73: filtro anti-spoofing GFI MailEssentials

2. Per abilitare il filtro anti-spoofing, selezionare **Abilita anti-spoofing**.

3. Nel campo **Server SMTP**, fornire l'indirizzo IP del server SMTP in cui GFI MailEssentials eseguirà il controllo degli indirizzi dei destinatari. Fornire inoltre una descrizione per il server nel campo **Descrizione:**.

> **NOTA**
> Il campo Server SMTP supporta i seguenti tipi di immissioni:
>
> » Indirizzo IP singolo
>
> » Intervallo CIDR (ad esempio, 192.0.2.1/24)

4. Per salvare i dati del server SMTP, fare clic su **Aggiungi server SMTP**.

> **NOTA**
> Per rimuovere i server SMTP precedentemente aggiunti, selezionare un server SMTP dall'Elenco di indirizzi IP autorizzati, quindi fare clic su **Rimuovi selezionati**.

Per impostazione predefinita, sono abilitate le opzioni **Utilizza indirizzi IP autorizzati dall'elenco server perimetrali** e **Non bloccare le connessioni autenticate**. Non è consigliabile disabilitarle.

> **NOTA**
> La casella di controllo **Non bloccare le connessioni autenticate** non si applica per Microsoft IIS e Microsoft Exchange 2003. È compatibile solo con Exchange 2007 o versioni successive. È compatibile solo con Exchange 2007 o versioni successive.

6.1.10 Greylist

Il filtro greylist blocca temporaneamente i messaggi di posta in arrivo ricevuti da mittenti sconosciuti. Normalmente, i sistemi di posta attendibili ritentano l'invio dopo alcuni minuti, gli spammer invece ignorano tali messaggi di errore.Se il messaggio viene ricevuto nuovamente dopo un periodo predefinito, la greylist:

» archivia i dettagli del mittente in un database, in modo che quando questi invierà un altro messaggio esso non verrà inserito nella greylist

» riceve il messaggio e procede con la scansione antispam

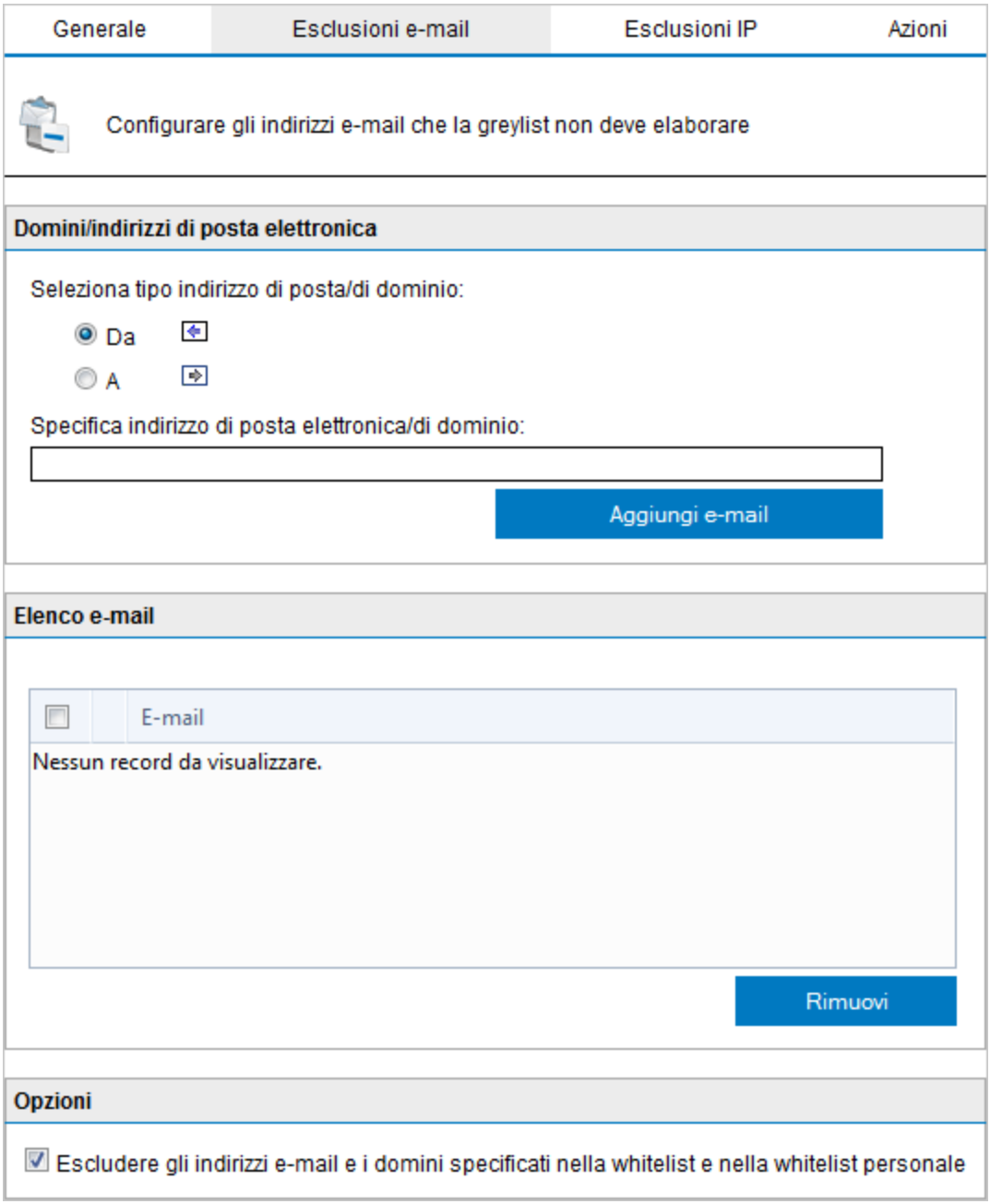
La greylist **NON** è abilitata per impostazione predefinita.

> **Note importanti**
>
> 1. Per abilitare la greylist, GFI MailEssentials deve essere installato sul server SMTP perimetrale. Per ulteriori informazioni, fare riferimento a http://go.gfi.com/?pageid=ME_GreylistSMTP
>
> 2. La greylist contiene gli elenchi di esclusione, in modo che indirizzi e-mail, domini e indirizzi IP specifici non siano inseriti nella greylist. Le esclusioni devono essere configurate quando:
>
> » non è possibile ritardare messaggi provenienti da determinati indirizzi e-mail, domini o indirizzi IP
>
> » non è possibile ritardare la posta indirizzata a un particolare utente locale

Configurazione greylist

1. Selezionare **Antispam > Filtri antispam > Greylist**.

2. Dalla scheda **Generale**, selezionare/deselezionare **Abilita greylist** per abilitare/disabilitare la greylist.



Schermata 74: Esclusioni e-mail

3. Per indicare gli indirizzi e-mail o i domini da non inserire nella greylist, selezionare la scheda **Esclusioni e-mail**. Nell'area **Modifica indirizzi**, specificare:

- l'indirizzo e-mail completo oppure
- gli indirizzi e-mail dell'intero dominio (ad esempio: *@trusteddomain.com) o
- il suffisso di un intero dominio (ad esempio: *@*.mil o *@*.edu)

Specificare anche se l'esclusione viene applicata ai mittenti (selezionare **Da (>)** o ai destinatari (selezionare **A (>)**) locali.

» **Esempio 1:** non inserire le e-mail nella greylist se il destinatario è administrator@mydomain.com, in modo che tutte le e-mail inviate a administrator@mydomain.com non vengano mai ritardate.

» **Esempio 2:** non inserire in greylist le e-mail se il dominio del mittente è trusteddomain.com (`*@trusteddomain.com`), in modo che le e-mail ricevute dal dominio trusteddomain.com non vengano mai ritardate.

Fare clic su **Aggiungi e-mail** per aggiungere l'esclusione.

> **NOTA**
> Per escludere dalla greylist (con conseguente ritardo) gli indirizzi e-mail e i domini inseriti nella whitelist e nella whitelist automatica, selezionare **Escludere gli indirizzi e-mail e i domini specificati nella whitelist**.

4. Per indicare gli indirizzi IP da escludere dalla greylist, selezionare la scheda **Esclusioni IP**. Fare clic su **Aggiungi IP** e indicare un IP da escludere.

5. Per escludere dalla greylist (con conseguente ritardo) gli indirizzi IP inseriti in whitelist, selezionare **Escludi indirizzi IP indicati nella whitelist**.

6. Per registrare le occorrenze della greylist in un file di registro, selezionare la scheda **Azioni** e quindi **Registra occorrenza regola nel seguente file**.

> **NOTA**
> I file di registro potrebbero diventare molto grandi. GFI MailEssentials supporta la rotazione del registro, durante la quale i nuovi file di registro vengono creati periodicamente oppure quando il file del registro raggiunge una determinata dimensione. Per abilitare la rotazione del file di registro, selezionare **Antispam > Impostazioni antispam**. Selezionare la scheda **Registrazione messaggi antispam**, fare clic su **Abilita rotazione file di registro** e indicare la condizione di rotazione.

7. Fare clic su **Applica**.

6.1.11 Rilevamento lingua

Determina la lingua del testo del corpo del messaggio ed è configurabile per il blocco di determinate lingue. GFI MailEssentials prende una parte del corpo del messaggio dell'e-mail e lo confronta con un motore della lingua integrato.

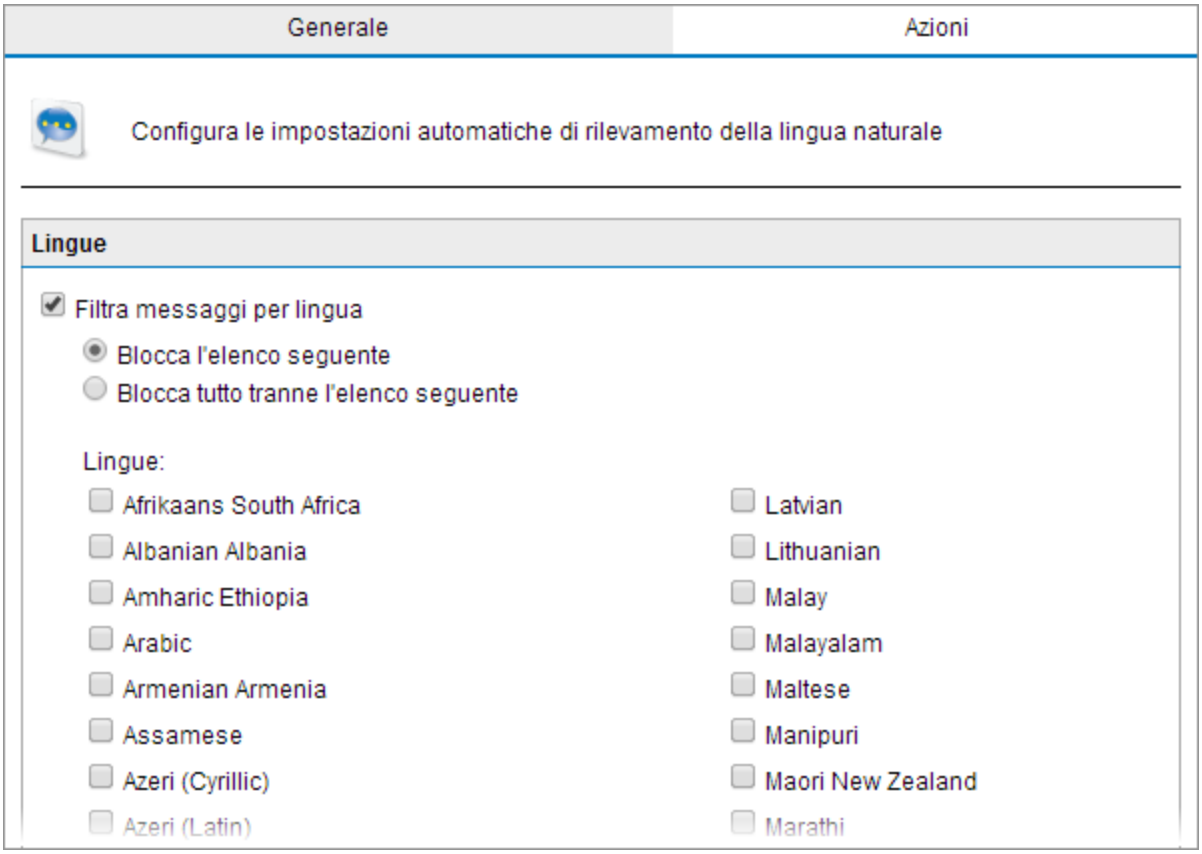
Configurare il filtro Rilevamento lingua per bloccare determinate lingue o consentirne solo alcune.

> **NOTA**
> Il filtro Rilevamento lingua è diverso dal filtro Controllo intestazione - Lingua perché analizza la lingua del testo del corpo del messaggio. Il filtro Controllo intestazione analizza la codifica (set di caratteri) dell'intestazione posta elettronica. Solitamente, i risultati del filtro Rilevamento lingua sono più affidabili.

Il filtro Rilevamento lingua **NON** è abilitato per impostazione predefinita al momento dell'installazione.

Configurazione rilevamento lingua

1. Accedere a **Antispam > Filtri antispam > Rilevamento lingua**.



Schermata 75: Opzioni di Rilevamento lingua

2. Dalla scheda **Generale**, selezionare/deselezionare **Filtra messaggi per lingua** per abilitare/disabilitare Rilevamento lingua.

3. Selezionare **Blocca l'elenco seguente** per scegliere le lingue da bloccare oppure **Blocca tutto tranne l'elenco seguente** per bloccare tutte le lingue ad eccezione di quelle selezionate.

4. Selezionare le lingue da bloccare/consentire dall'area **Lingue**.

5. Per selezionare le azioni da effettuare sui messaggi identificati come spam, fare clic sulla scheda **Azioni**. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148).

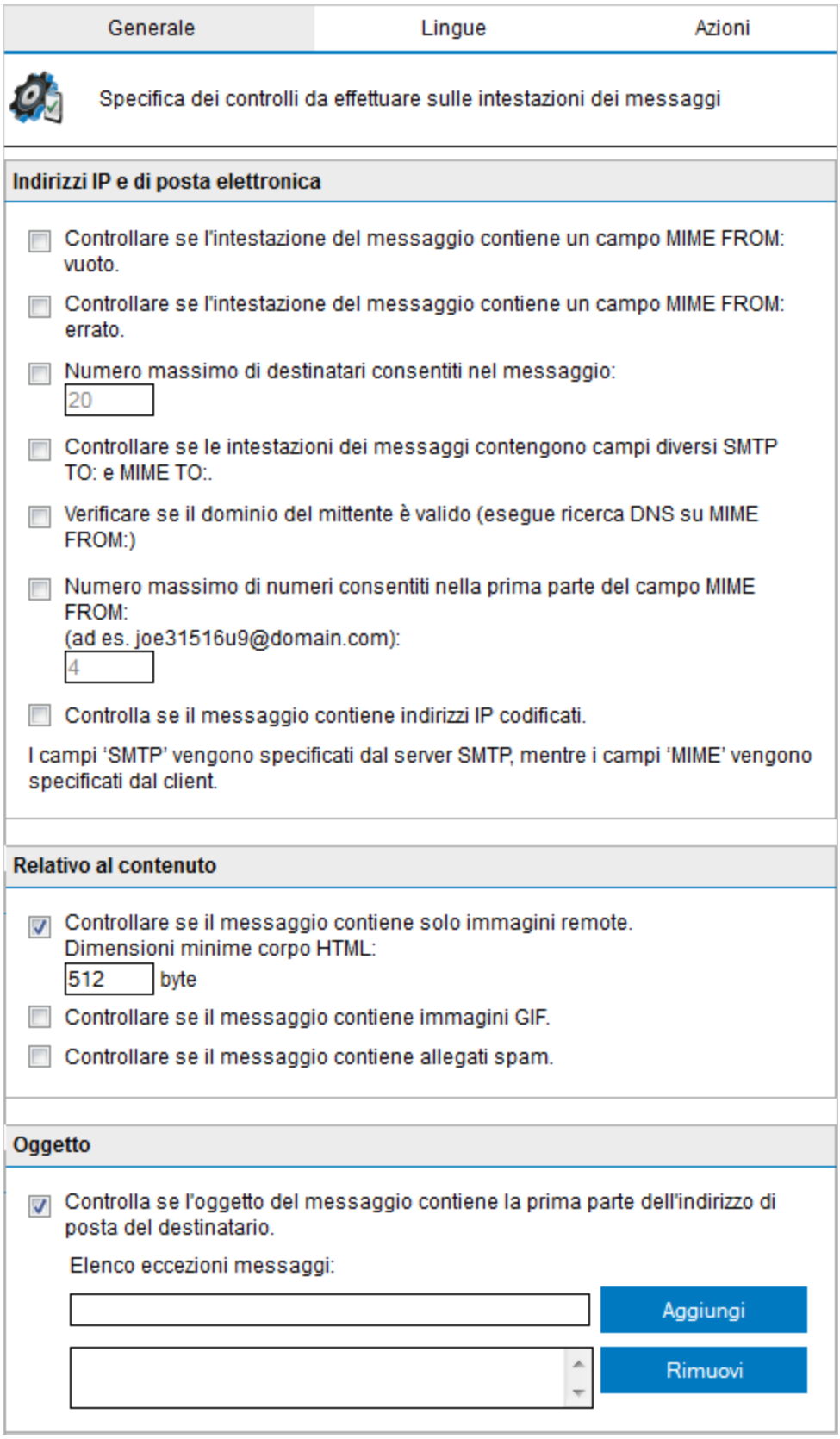
6. Fare clic su **Applica**.

6.1.12 Controllo intestazione

Il filtro Controllo intestazione analizza l'intestazione e-mail per identificare i messaggi spam.

Configurazione controllo intestazione

1. Selezionare **Antispam > Filtri antispam > Controllo intestazione**.


Generale
Lingue
Azioni
Specifica dei controlli da effettuare sulle intestazioni dei messaggi
Indirizzi IP e di posta elettronica
Controllare se l'intestazione del messaggio contiene un campo MIME FROM: vuoto.
Controllare se l'intestazione del messaggio contiene un campo MIME FROM: errato.
Numero massimo di destinatari consentiti nel messaggio:
20
Controllare se le intestazioni dei messaggi contengono campi diversi SMTP TO: e MIME TO:.
Verificare se il dominio del mittente è valido (esegue ricerca DNS su MIME FROM:)
Numero massimo di numeri consentiti nella prima parte del campo MIME FROM:
(ad es. joe31516u9@domain.com):
4
Controlla se il messaggio contiene indirizzi IP codificati.
I campi 'SMTP' vengono specificati dal server SMTP, mentre i campi 'MIME' vengono specificati dal client.
Relativo al contenuto
Controllare se il messaggio contiene solo immagini remote.
Dimensioni minime corpo HTML:
512
byte
Controllare se il messaggio contiene immagini GIF.
Controllare se il messaggio contiene allegati spam.
Oggetto
Controlla se l'oggetto del messaggio contiene la prima parte dell'indirizzo di posta del destinatario.
Elenco eccezioni messaggi:
Aggiungi
Rimuovi

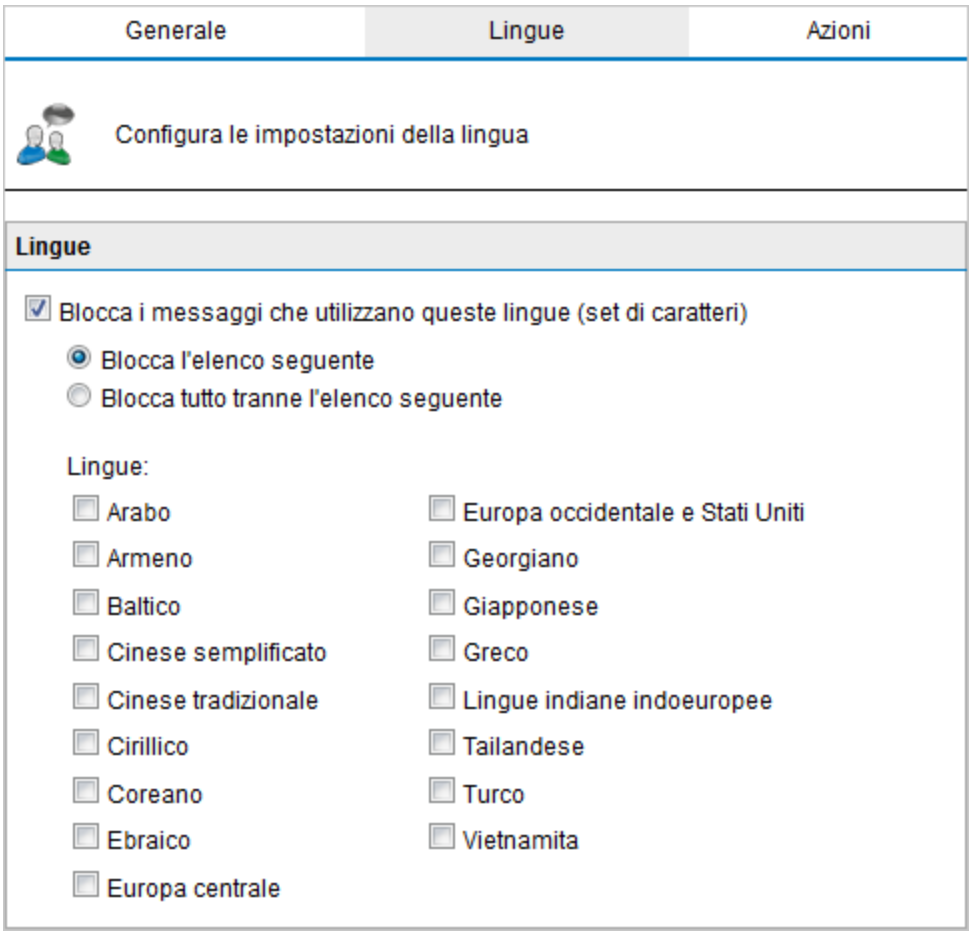
Schermata 76: opzioni di Controllo intestazione

2. Abilitare, disabilitare o configurare i seguenti parametri:

Opzione	Descrizione
Controllare se l'intestazione del messaggio contiene un campo MIME FROM: vuoto.	Controllare se il mittente si è identificato nel campo Da:. Se il campo è vuoto, il messaggio verrà contrassegnato come spam.
Controllare se l'intestazione del messaggio contiene un campo MIME FROM: errato.	Controlla se il campo "MIME from" è nella notazione corretta definita in RFC.
Numero massimo di destinatari consentiti nel messaggio	Identifica la posta con grandi quantitativi di destinatari e li contrassegna come SPAM.
Controllare se le intestazioni dei messaggi contengono campi diversi SMTP TO: e MIME TO:.	Controlla se i campi SMTP TO: e MIME TO: negli indirizzi di posta sono gli stessi. Il server della posta degli spammer deve includere un indirizzo SMTP to:. Tuttavia, l'indirizzo di posta MIME to: spesso non è incluso o è diverso. **NOTA:** Questa caratteristica identifica molta spam, tuttavia alcuni server di elenco non includono nemmeno MIME to:. Pertanto, per utilizzare questa funzione, si consiglia di inserire nella whitelist l'indirizzo del mittente.
Verificare se il dominio del mittente è valido (esegue ricerca DNS su MIME FROM:)	Esegue una ricerca DNS sul dominio nel campo MIME from e verifica la validità del dominio. **NOTA:** assicurarsi che il server DNS sia correttamente configurato per evitare timeout e rallentamenti del flusso di posta.
Numero massimo di numeri consentiti nella prima parte del campo MIME FROM:.	Identifica la presenza di numeri nel campo "MIME from". Spesso gli spammer utilizzano strumenti che creano automaticamente indirizzi "reply-to:" univoci tramite i numeri presenti nell'indirizzo.
Controlla se il messaggio contiene indirizzi IP codificati.	Controlla l'intestazione e il corpo del messaggio alla ricerca di URL con IP codificato esadecimale/ottale (http://0072389472/hello.com) o con una combinazione di nomeutente/password (ad esempio www.citibank.com@scammer.com). I seguenti esempi sono contrassegnati come spam: » http://12312 » www.microsoft.com:hello%01@123123
Controlla se il messaggio contiene solo immagini remote. Dimensioni minime corpo HTML	Contrassegna come spam i messaggi contenenti solamente immagini remote e una quantità minima di testo. Aiuta nell'identificare la spam del tipo 'posta solo immagine'.
Controlla se il messaggio contiene immagini GIF.	Controlla se la posta contiene una o più immagini GIF incorporate. Le immagini GIF incorporate sono spesso utilizzate per evitare i filtri antispam. **IMPORTANTE:** dato che alcuni messaggi attendibili contengono immagini GIF incorporate, questa opzione può portare a falsi positivi.
Controllare se il messaggio contiene allegati spam.	Controlla se negli allegati di posta sono presenti proprietà comuni agli allegati inviati nella posta antispam. Ciò aiuta a rimanere aggiornati con le ultime tecnologie utilizzate dagli spammer per l'uso di allegati per l'invio di spam.
Controlla se l'oggetto del messaggio contiene la prima parte dell'indirizzo di posta del destinatario.	Identifica il messaggio spam personalizzato, in cui gli spammer includono di frequente nell'oggetto la prima parte dell'indirizzo di posta del destinatario.

3. Per abilitare il rilevamento della lingua, dalla scheda **Lingua**, selezionare **Blocca i messaggi che utilizzano queste lingue**.

> **NOTA**
> il filtro Controllo intestazione - Lingua è diverso dal filtro Rilevamento lingua perché analizza la codifica (set di caratteri) dell'intestazione posta elettronica. Rilevamento lingua analizza la lingua del testo del corpo del messaggio. Solitamente, i risultati del filtro Rilevamento lingua sono più affidabili.



Schermata 77: Rilevamento lingua

4. Selezionare **Blocca l'elenco seguente** per scegliere le lingue da bloccare oppure **Blocca tutto tranne l'elenco seguente** per bloccare tutte le lingue ad eccezione di quelle selezionate.

5. Selezionare le lingue da bloccare/consentire dall'area **Lingue**.

6. Per selezionare le azioni da effettuare sui messaggi identificati come spam, fare clic sulla scheda **Azioni**. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148).

7. Fare clic su **Applica**.

6.1.13 Controllo parole chiave spam

Questo filtro consente l'identificazione dello spam sulla base di parole chiave all'interno del messaggio ricevuto.

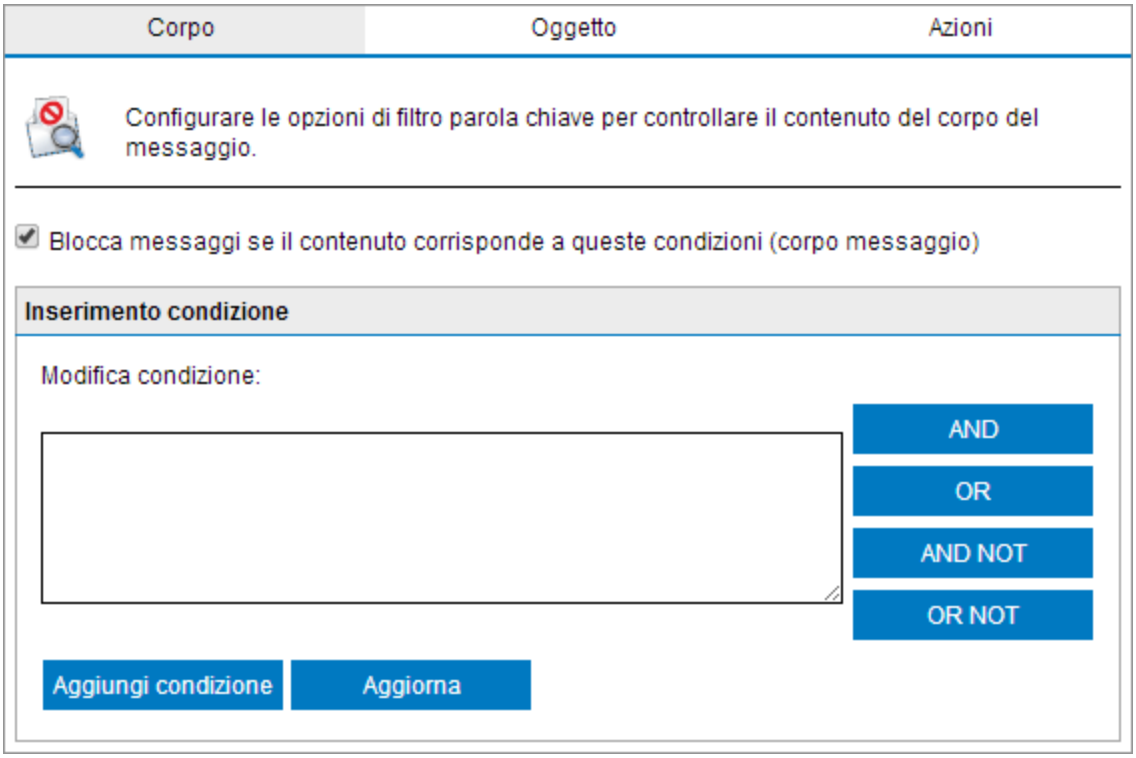
Questo filtro **NON** è abilitato per impostazione predefinita al momento dell'installazione di GFI MailEssentials.

> **NOTA**
> Questo filtro controlla solo il contenuto del messaggio alla ricerca di testo che identifica il messaggio come spam. Per un filtro del contenuto completo del messaggio (ad esempio per bloccare contenuti razzisti o offensivi), usare l'opzione Filtro parole chiave all'interno del nodo Filtro contenuti.

Aggiunta controllo parole chiave di spam

1. Selezionare **Antispam > Filtri antispam > Controllo parole chiave spam.**

2. Per abilitare il Controllo parola chiave spam sul corpo del messaggio, nella scheda **Corpo**, selezionare **Blocca messaggi se il contenuto corrisponde a queste condizioni (corpo messaggio).**



Schermata 78: proprietà di Controllo parole chiave spam

3. Nell'area **Inserimento condizione**, immettere una parola chiave o combinazione di parole chiave che devono essere bloccate dal filtro. Per configurare condizioni specifiche, utilizzare gli operatori 'AND', 'OR', 'AND NOT' e 'OR NOT'.

Ad esempio:

- `Sport basket` - GFI MailEssentials blocca i messaggi con la frase `Sport basket`. Solo questa frase attiverebbe la regola, non la parola `basket` O `sport` separate da altre parole.
- `Basket E baseball` - GFI MailEssentials blocca i messaggi con entrambe le parole nel messaggio di posta. I messaggi con solo `basket` o `baseball` non verranno bloccati.

4. Selezionare **Rileva solo parole intere** per cercare in modo specifico parole intere ed evitare il blocco di parole che fanno parte di altre. Ad esempio, abilitando questa opzione non verrebbe bloccata la parola 'MSExchange', a prescindere dal fatto che la parola 'sex' faccia parte di 'MSExchange'.

5. Selezionare la scheda **Oggetto**, quindi fare clic su **Blocca messaggi se il contenuto corrisponde a queste condizioni (oggetto messaggio)** per abilitare il Controllo parole chiave spam nell'oggetto del messaggio.

6. Nell'area **Inserimento condizione**, immettere una parola chiave o combinazione di parole chiave che devono essere bloccate dal filtro. Per configurare condizioni specifiche, utilizzare gli operatori 'AND', 'OR', 'AND NOT' e 'OR NOT'.

7. Selezionare **Applicare l'elenco di parole chiave anche per scansionare i nomi visualizzati dei mittenti** per controllare il nome visualizzato dell'indirizzo di posta del mittente, il quale può contenere parole chiave di spam. Ad esempio, lo spam Viagra, che spesso presenta mittenti falsificati e la parola Viagra si trova nell'oggetto.

8. Per selezionare le azioni da effettuare sui messaggi identificati come spam, fare clic sulla scheda **Azioni**. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148).

9. Fare clic su **Applica**.

Rimozione delle condizioni

Per rimuovere una condizione Controllo parole chiave spam:

1. Dall'area **Elenco condizioni** all'interno della scheda **Corpo** o **Oggetto**, selezionare una o più condizioni da rimuovere.

> **NOTA**
> Per trovare la condizione da rimuovere, utilizzare i comandi posti sotto l'elenco di condizioni per spostarsi tra le pagine che le elencano.

2. Fare clic su **Rimuovi** e su **Applica**.

Importazione ed esportazione delle condizioni

Per esportare più condizioni:

1. Dall'area **Elenco condizioni** all'interno della scheda **Corpo** o **Oggetto**, selezionare una o più condizioni da esportare.

> **NOTA**
> Per trovare la condizione da esportare, utilizzare i comandi posti sotto l'elenco di condizioni per spostarsi tra le pagine che le elencano.

2. Nella finestra di dialogo **Download file**, selezionare **Salva** quindi scegliere una cartella in cui salvare il file di esportazione.

Per importare le condizioni:

1. Dall'area **Elenco condizioni** all'interno della scheda **Corpo** o **Oggetto**, digitare la cartella e il nome file del file da importare.

2. Fare clic su **Importa**.

6.1.14 Analisi bayesiana

Un filtro antispam che può essere addestrato per determinare con precisione se un messaggio è spam in base a quanto rilevato in precedenza.

Il presente manuale contiene anche informazioni sul funzionamento del filtro bayesiano e sulle modalità di addestramento dello stesso. Per ulteriori informazioni, fare riferimento a Appendice - Filtro bayesiano (pagina 292).

L'analisi bayesiana **NON** è abilitata per impostazione predefinita.

IMPORTANTE

Abiliare l'apprendimento dai messaggi in uscita e attendere almeno una settimana prima di attivare il filtro. È necessario eseguire tale operazione preliminare, dato che il filtro bayesiano raggiunge il tasso massimo di rilevazione quando si adatta alla struttura della posta dell'utente.

Configurazione del filtro bayesiano

La configurazione del filtro bayesiano richiede due passaggi:

Passaggio 1: Addestramento del filtro bayesiano

Passaggio 2: Abilitazione del filtro bayesiano

Passaggio 1: addestramento del filtro bayesiano

Il filtro bayesiano può essere addestrato con due modalità:

Metodo 1: in automatico, sulla base dei messaggi di posta in uscita.

GFI MailEssentials elabora la posta attendibile (ham) effettuando la scansione della posta in uscita. Il filtro bayesiano può essere abilitato dopo che ha raccolto almeno 500 messaggi di posta in uscita (se si invia principalmente posta in lingua inglese) oppure 1000 messaggi in uscita (se si spedisce posta non in lingua inglese).

A tale scopo, procedere come segue:

1. Accedere a **Antispam > Filtri antispam > Analisi bayesiana**.

2. Selezionare **Apprendi automaticamente da posta elettronica in uscita**.

3. Fare clic su **Applica**.

Metodo 2: manualmente, sulla base della posta esistente.

Copiare 500-1000 messaggi dalla posta inviata alla sottocartella **Messaggio attendibile** delle cartelle pubbliche di **Cartelle anti-spam di GFI**. In tal modo, il filtro bayesiano viene addestrato come con la posta in uscita.

NOTA

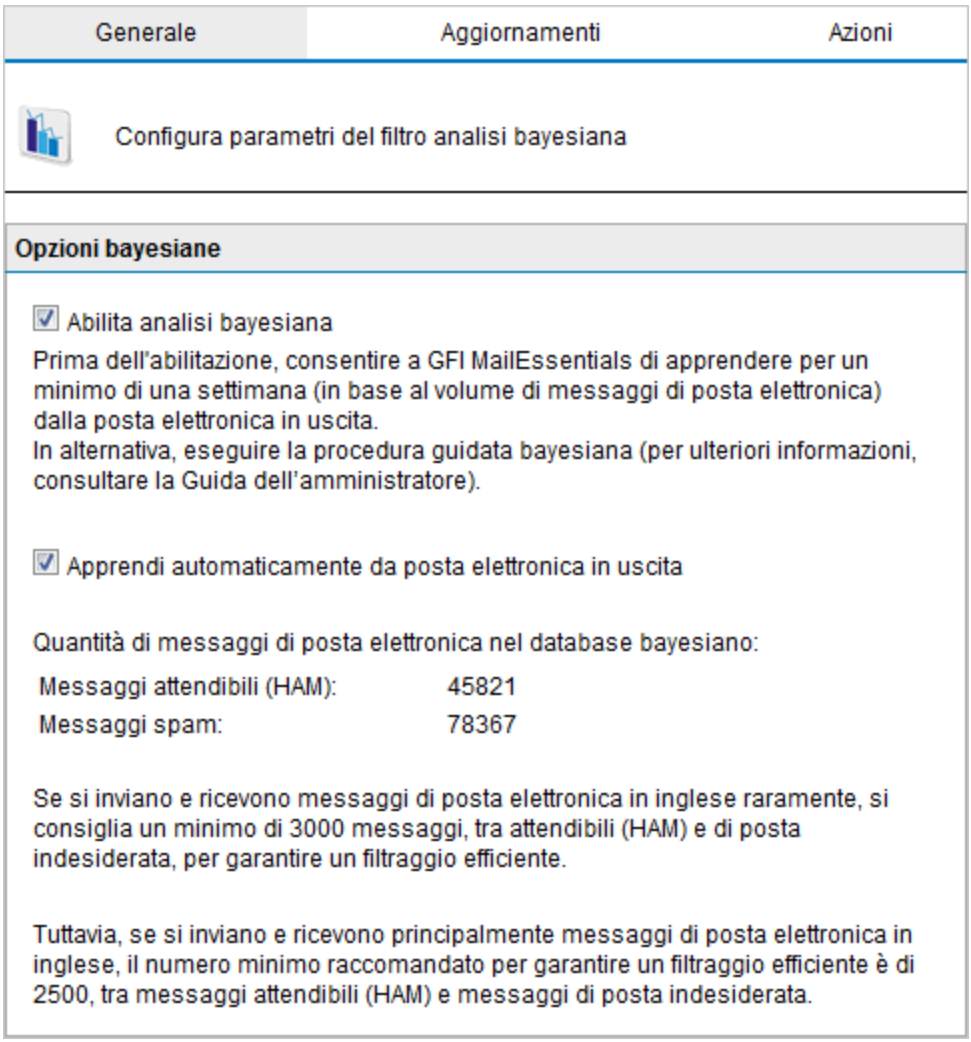
Per poter utilizzare questa opzione, deve essere abilitata Scansione cartella pubblica. Per ulteriori informazioni, fare riferimento a Scansione cartella pubblica (pagina 170).

Passaggio 2: abilitazione del filtro bayesiano

Dopo aver addestrato il filtro bayesiano, dovrà essere abilitato.

1. Dalla console di configurazione di GFI MailEssentials, accedere a **Antispam > Filtri antispam > Analisi bayesiana**.

2. Dalla scheda **Generale**, selezionare **Abilita analisi bayesiana**.


Generale
Aggiornamenti
Azioni
Configura parametri del filtro analisi bayesiana
Opzioni bayesiane
Abilita analisi bayesiana
Prima dell'abilitazione, consentire a GFI MailEssentials di apprendere per un minimo di una settimana (in base al volume di messaggi di posta elettronica) dalla posta elettronica in uscita.
In alternativa, eseguire la procedura guidata bayesiana (per ulteriori informazioni, consultare la Guida dell'amministratore).
Apprendi automaticamente da posta elettronica in uscita
Quantità di messaggi di posta elettronica nel database bayesiano:
Messaggi attendibili (HAM): 45821
Messaggi spam: 78367
Se si inviano e ricevono messaggi di posta elettronica in inglese raramente, si consiglia un minimo di 3000 messaggi, tra attendibili (HAM) e di posta indesiderata, per garantire un filtraggio efficiente.
Tuttavia, se si inviano e ricevono principalmente messaggi di posta elettronica in inglese, il numero minimo raccomandato per garantire un filtraggio efficiente è di 2500, tra messaggi attendibili (HAM) e messaggi di posta indesiderata.

Schermata 79: proprietà analisi bayesiana

3. Nella scheda **Aggiornamenti**, configurare la frequenza degli aggiornamenti al database antispam abilitando **Controlla automaticamente aggiornamenti** e configurando un intervallo orario.

> **NOTA**
> Per scaricare immediatamente gli aggiornamenti disponibili, fare clic su **Scarica aggiornamenti adesso...**.

> **NOTA**
> Gli aggiornamenti possono essere scaricati utilizzando un server proxy. Per ulteriori informazioni, fare riferimento a Impostazioni proxy (pagina 242).

4. Per selezionare le azioni da effettuare sui messaggi identificati come spam, fare clic sulla scheda **Azioni**. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148).

5. Fare clic su **Applica**.

NOTA

GFI MailEssentials offre inoltre una procedura guidata analisi bayesiana per consentire all'utente di di addestrare il filtro di analisi bayesiana da un computer diverso da quello dove è installato GFI MailEssentials. Per ulteriori informazioni, fare riferimento a Addestramento del filtro analisi bayesiana (pagina 293).

6.1.15 Whitelist

NOTA

La whitelist interessa solo i filtri antispam, non la sicurezza e-mail né tantomeno il filtro contenuti.

La whitelist contiene gli elenchi dei criteri che identificano la posta attendibile. Le e-mail che rispettano tali criteri non saranno scansionate dai filtri antispam e verranno sempre recapitate al destinatario. Le e-mail possono essere inserite nella whitelist mediante i seguenti criteri:

- indirizzo e-mail, dominio di posta elettronica o indirizzo IP del mittente
- mittenti a cui è stata precedentemente inviata un'e-mail (whitelist automatica)
- destinatario (esclude il filtro della posta proveniente da indirizzi e-mail locali)
- parole chiave nel corpo del messaggio o nell'oggetto

Le funzioni di whitelist e whitelist automatica sono abilitate per impostazione predefinita.

Note importanti

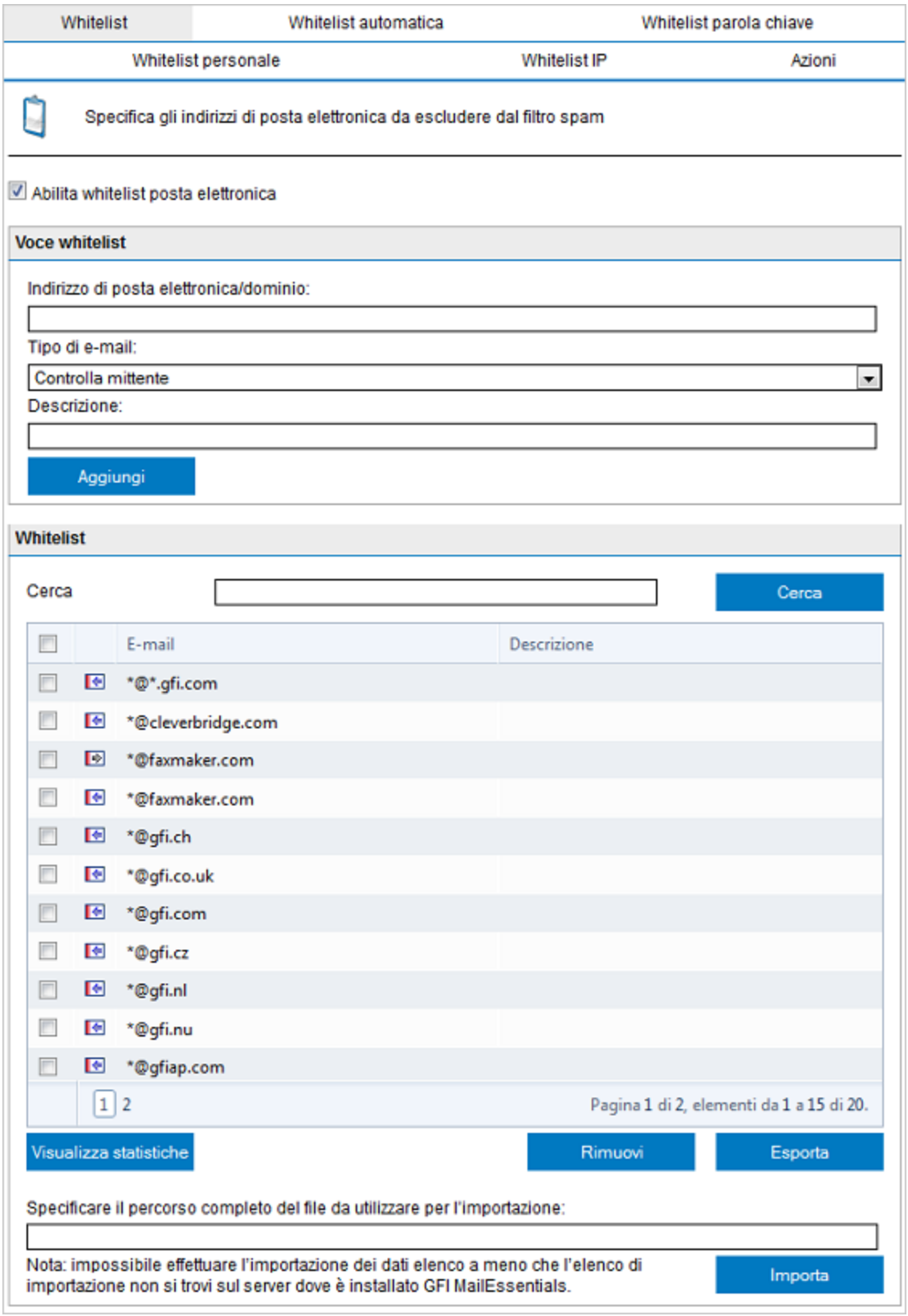
L'utilizzo della funzione di whitelist automatica è particolarmente consigliato, poiché elimina una percentuale elevata di falsi positivi.

In Whitelist parola chiave, si consiglia di aggiungere i termini che gli spammer non utilizzano e che fanno riferimento al proprio tipo di attività, ad esempio i nomi dei prodotti. L'inserimento di numerose parole chiave incrementa le possibilità che le e-mail non vengano filtrate da GFI MailEssentials e che siano recapitate nelle cassette postali degli utenti.

L'inserimento nella whitelist di un utente interno rende vano lo scopo di un filtro anti-spoofing. Per ulteriori informazioni, fare riferimento a Anti-spoofing (pagina 129).

Configurazione whitelist

1. Fare clic su **AntiSpam > Whitelist**.



Schermata 80: scheda Whitelist

2. Dalla scheda **Whitelist**, configurare gli indirizzi e-mail e i domini da inserire nella whitelist. Per abilitare/disabilitare la whitelist, selezionare/deselezionare **Abilita whitelist posta elettronica**. Effettuare le azioni indicate di seguito:

Azione	Descrizione
Aggiunta voce whitelist	1. In **Dominio/indirizzo di posta elettronica**, fornire l'indirizzo di posta/dominio da inserire nella whitelist. **Ad esempio**: . *@companysupport.com o. *@*.edu. 2. In **Tipo di e-mail**, indicare il campo intestazione e-mail valido per i messaggi da inserire nella whitelist. **NOTA** Per ulteriori informazioni sulla differenza tra SMTP e MIME fare riferimento a: http://go.gfi.com/?pageid=ME_DifferenceSMTPMIME 3. (Facoltativo) È anche possibile aggiungere una descrizione alla voce nel campo **Descrizione**. 4. Fare clic su **Aggiungi**.
Rimozione voci whitelist	1. Selezionare uno o più voci whitelist dall'elenco **Whitelist**. 2. Fare clic su **Rimuovi**.
Ricerca di una voce whitelist	1. In **Cerca**, digitare i dettagli della voce di whitelist da cercare. 2. Per visualizzare l'elenco dei termini corrispondenti, fare clic su **Cerca**.
Visualizza statistiche	Per visualizzare il numero totale di messaggi bloccati per voce di whitelist, utilizzare il pulsante **Visualizza statistiche**.
Importazione voci whitelist	1. Specificare il percorso completo e nome del file da utilizzare per l'importazione dei dati precedentemente esportati. 2. Per importare le voci, fare clic su **Importa**.
Esportazione voci whitelist	Per esportare l'elenco attuale di voci whitelist in un file XML, fare clic su **Esporta**.

3. Fare clic sulla scheda **Whitelist automatica** per configurare le seguenti opzioni:

Opzione	Descrizione
Popola automaticamente Whitelist automatica:	Selezionando questa opzione, gli indirizzi e-mail di destinazione dei messaggi in uscita vengono aggiunti automaticamente alla whitelist automatica.
Abilita Whitelist automatica di posta elettronica	Per abilitare la whitelist automatica, selezionare questa opzione. I mittenti dei messaggi in entrata verranno confrontati con la whitelist automatica. Se il mittente è presente nell'elenco, il messaggio viene inoltrato direttamente nella casella di posta in arrivo del destinatario.
Numero massimo voci consentite in Whitelist automatica:	Specificare il numero di voci consentite nella whitelist automatica. Quando si supera il limite specificato, le voci più vecchie e meno usate vengono automaticamente sostituite con delle nuove. **NOTA** L'immissione di un valore superiore a quello predefinito di 30.000 può influenzare negativamente le prestazioni di GFI MailEssentials.

4. Dalla scheda **Whitelist parola chiave**, indicare le parole chiave che contrassegnano i messaggi come validi:

Opzione	Descrizione
Abilita la whitelist delle parole chiave nel corpo del messaggio di posta elettronica	Selezionare questa opzione per cercare le parole chiave nel corpo del messaggio che identificano un messaggio come valido. Aggiungere le parole chiave all'elenco **Parole chiave nel corpo**. È anche possibile importare o esportare elenchi di parole chiave da/a un file XML.

Opzione	Descrizione
Abilita la whitelist delle parole chiave nell'oggetto del messaggio di posta elettronica	Selezionare questa opzione per cercare le parole chiave nell'oggetto corpo del messaggio che identificano un messaggio come valido. Aggiungere le parole chiave all'elenco **Parole chiave nell'oggetto**. È anche possibile importare o esportare elenchi di parole chiave da/a un file XML.
Rileva solo parole intere (parole/frasi in oggetto/corpo)	Al momento di selezionare questa opzione, vengono confrontate solo le parole intere della whitelist parole chiave che identificano un messaggio come valido.

5. Dalla scheda **Whitelist IP**, configurare quanto segue:

Opzione	Descrizione
Abilita Whitelist IP	Selezionare la scheda per consentire i messaggi ricevuti da indirizzi IP specifici.
Aggiunta voci whitelist IP	1. Indicare: » **Computer singolo/CIDR**: Immettere un singolo indirizzo IP utilizzando la notazione CIDR. » **Gruppo di computer**: Indicare **Indirizzo subnet** e **Subnet Mask** del gruppo di IP da inserire in whitelist. 2. (Facoltativo) Aggiungere una **Descrizione**. 3 Fare clic su **Aggiungi**.
Rimozione voci whitelist IP	Selezionare gli IP da rimuovere e fare clic su **Rimuovi**.

6. Per abilitare/disabilitare la registrazione delle occorrenze whitelist in un file, fare clic sulla scheda **Azioni**. Fornire un percorso/cartella dove archiviare il file di registro generato.

7. Fare clic su **Applica**.

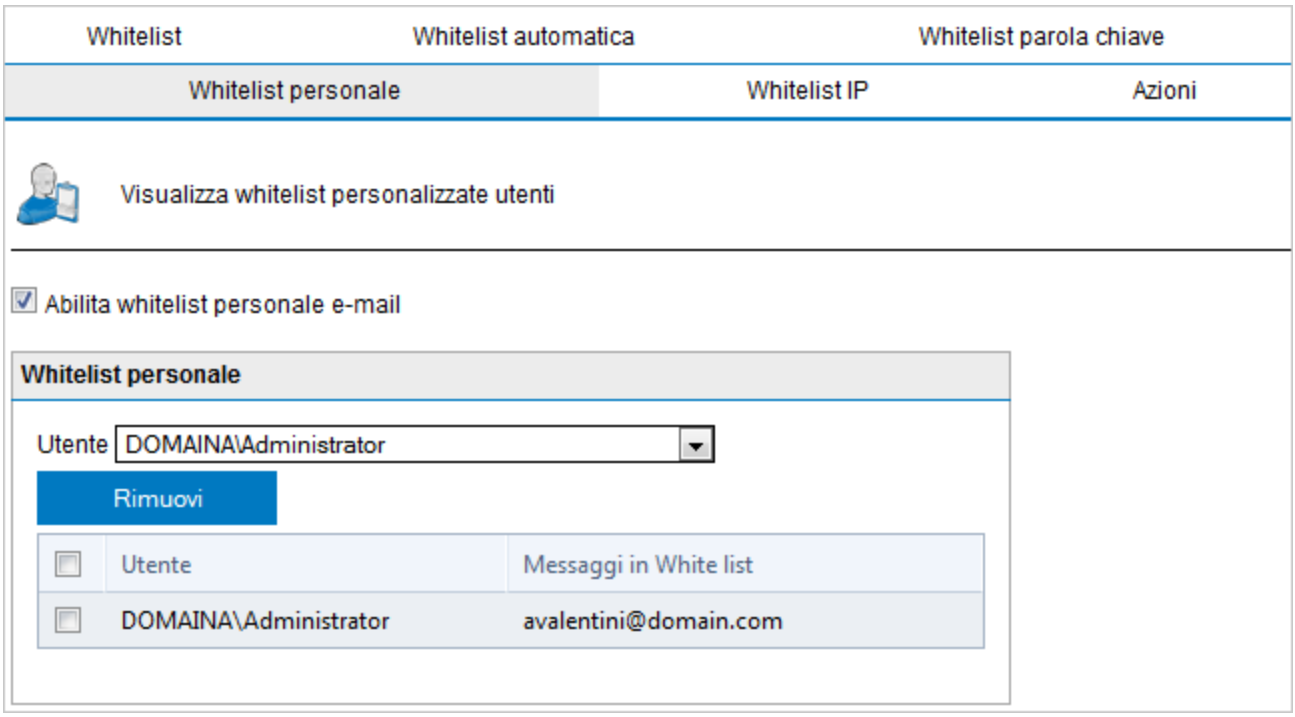
Whitelist personale

La whitelist personale è una whitelist aggiuntiva che si integra una whitelist globale. Disabilitata per impostazione predefinita, la whitelist personale può essere abilitata per gli utenti, consentendo così loro di aggiungere indirizzi di posta specifici a una whitelist personale che possano gestire. Per ulteriori informazioni, fare riferimento a Azioni utente finale (pagina 21).

Per gli scopi di gestione, gli amministratori possono anche rimuovere indirizzi di posta specifici che gli utenti hanno aggiunto alla loro whitelist personale.

Abilitazione/disabilitazione whitelist personali

1. Fare clic su **Antispam** > **Whitelist**.



Schermata 81: whitelist personale

2. Selezionare la scheda **Whitelist personale** e selezionare o deselezionare **Abilita whitelist personale e-mail** per abilitare o disabilitare la funzione della whitelist personale.

3. Fare clic su **Applica**.

Rimozione degli utenti dalla whitelist personale degli utenti

1. Fare clic su **Antispam > Whitelist** e selezionare la scheda **Whitelist personale**.

2. Dall'elenco a discesa **Utente**, selezionare l'utente di cui eliminare un indirizzo di posta.

3. Selezionare un indirizzo di posta dall'elenco. Fare clic su **Rimuovi**.

4. Fare clic su **Applica**.

6.1.16 Nuovi mittenti

Il filtro Nuovi mittenti identifica i messaggi di posta elettronica inviati da mittenti ai quali non sono mai stati inviati messaggi. Questi mittenti vengono identificati attraverso il riferimento ai dati raccolti nella whitelist.

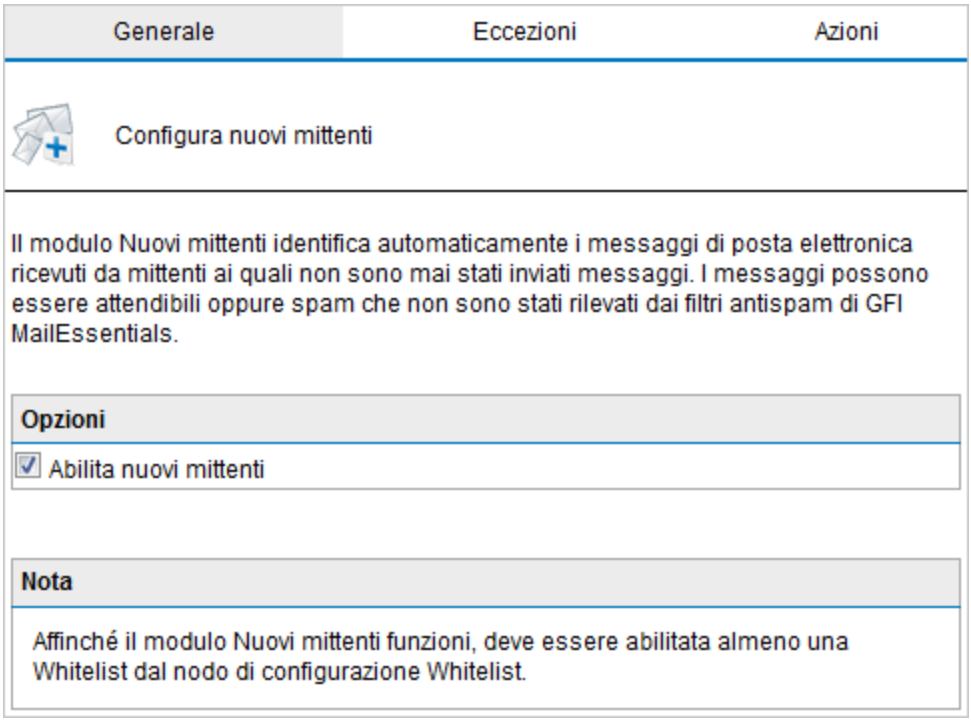
Il filtro Nuovi mittenti viene attivato solo per i messaggi dove non viene rilevata spam e il cui mittente non è presente in nessuna whitelist.

Questo filtro **NON** è abilitato per impostazione predefinita.

Importante
Per poter utilizzare la funzione Nuovi mittenti, è necessario abilitare almeno una delle whitelist disponibili. Nell'assenza delle funzioni Whitelist (se non dovesse essere rilevata spam da altri filtri), i messaggi ricevuti verranno recapitati alla posta in arrivo del destinatario. **SOLO** i messaggi in cui non è stata rilevata spam e i cui mittenti non sono presenti nella whitelist vengono consegnati nella cartella Nuovi mittenti.

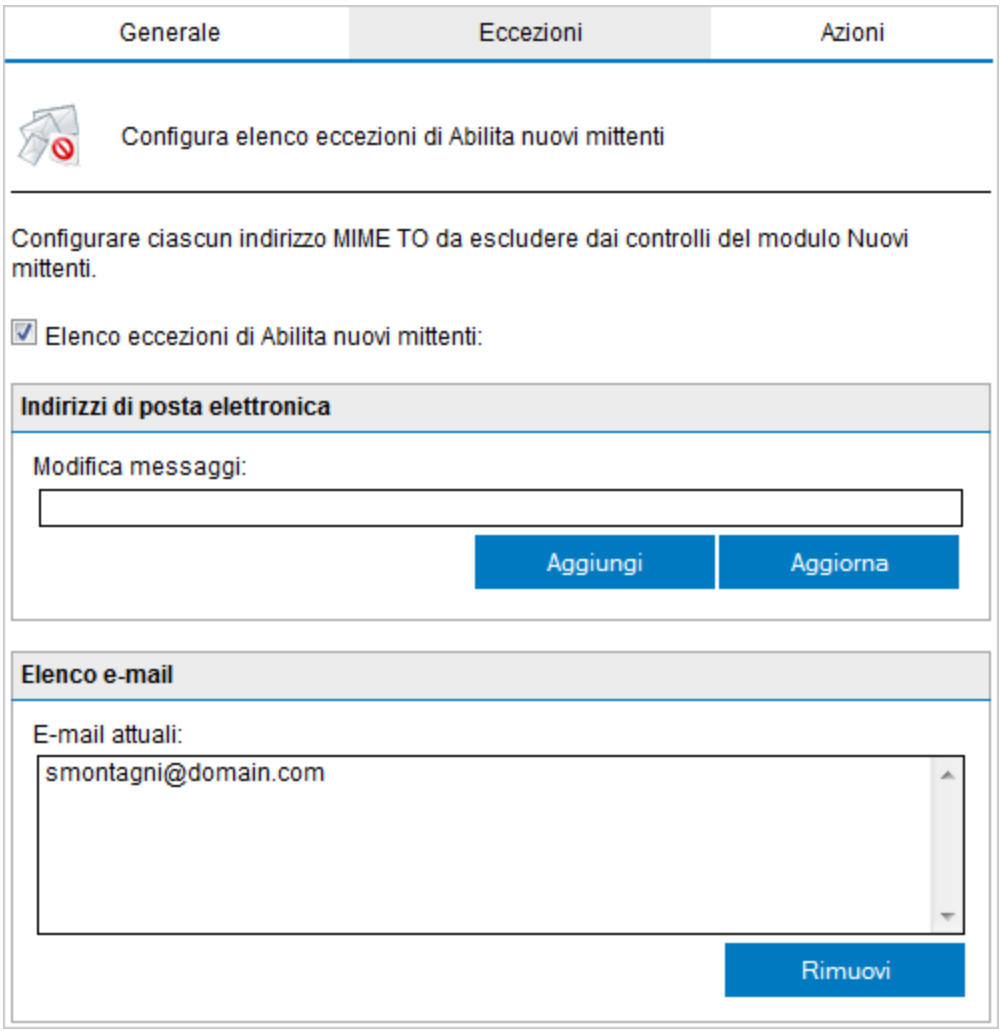
Configurazione filtro Nuovi mittenti

1. Selezionare **Antispam > Nuovi mittenti**.


Generale
Eccezioni
Azioni
Configura nuovi mittenti
Il modulo Nuovi mittenti identifica automaticamente i messaggi di posta elettronica ricevuti da mittenti ai quali non sono mai stati inviati messaggi. I messaggi possono essere attendibili oppure spam che non sono stati rilevati dai filtri antispam di GFI MailEssentials.
Opzioni
Abilita nuovi mittenti
Nota
Affinché il modulo Nuovi mittenti funzioni, deve essere abilitata almeno una Whitelist dal nodo di configurazione Whitelist.

Schermata 82: scheda Generale di Nuovi mittenti

2. Nella scheda **Generale**, selezionare **Abilita nuovi mittenti** per consentire il controllo di nuovi mittenti su tutti i messaggi in entrata.



Schermata 83: eccezioni Nuovi mittenti

3. Dalla scheda **Eccezioni**, configurare i mittenti/destinatari i cui messaggi sono esclusi dal controllo Nuovi mittenti.

Opzione	Descrizione
Elenco eccezioni di Abilita nuovi mittenti	Per abilitare l'elenco eccezioni, selezionare questa opzione.
Aggiungi eccezione	Digitare un indirizzo e-mail da escludere e fare clic su **Aggiungi**. Ripetere la procedura per ciascun indirizzo da aggiungere.
Modifica eccezione	1. Selezionare un'eccezione da **Elenco e-mail**. 2. Modificare l'indirizzo e-mail. 3. Fare clic su **Aggiorna**.
Elimina eccezione	Selezionare un'eccezione da **Elenco e-mail** e fare clic su **Rimuovi**.

4. Per selezionare le azioni da effettuare sui messaggi identificati come spam, fare clic sulla scheda **Azioni**. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148).

5. Fare clic su **Applica**.

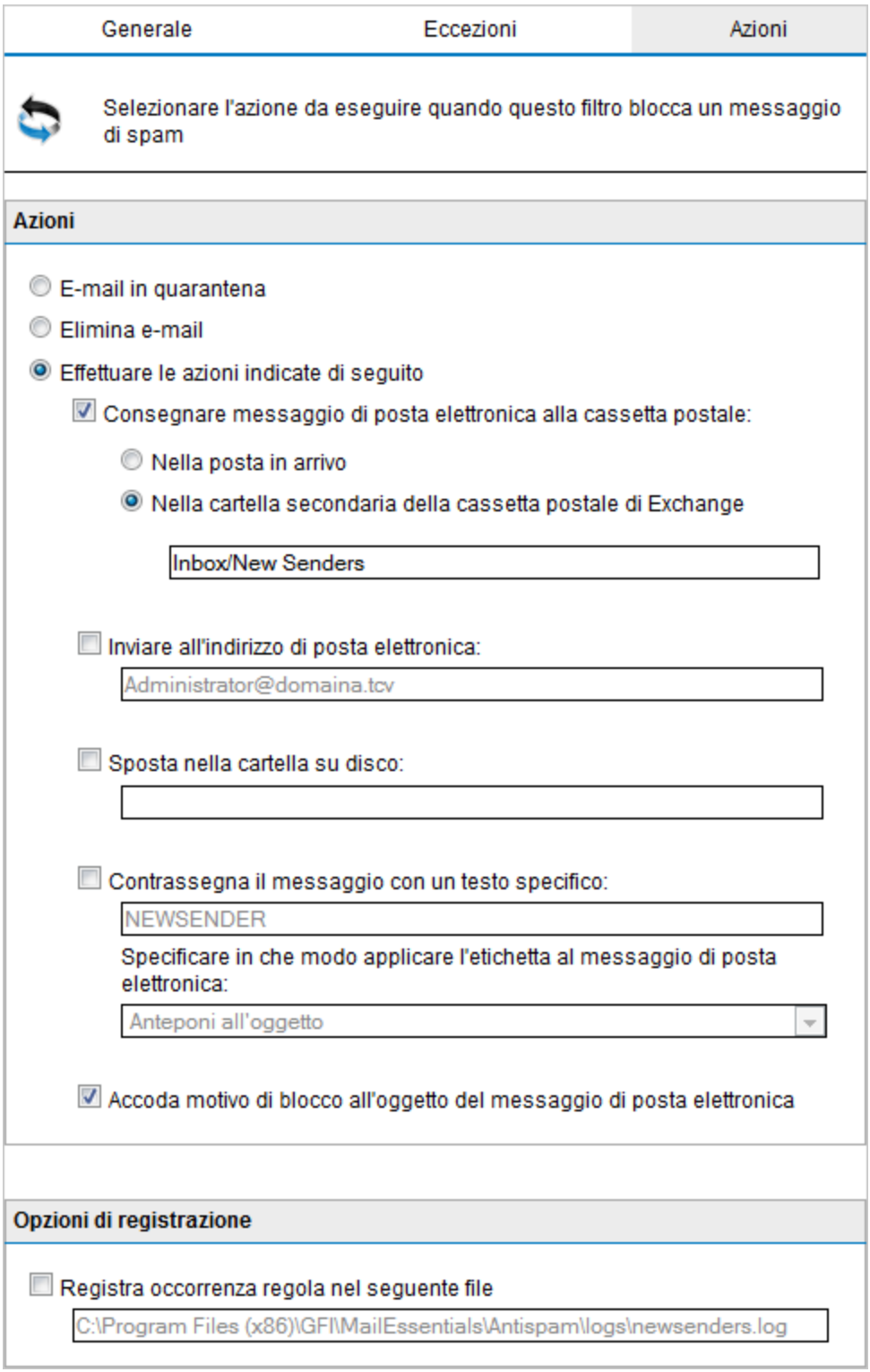
6.2 Operazioni antispam - cosa fare con lo spam.

La scheda **Azioni** delle proprietà dei filtri antispam definisce le operazioni da eseguire con i messaggi contrassegnati come spam. Per ciascun filtro antispam è possibile definire operazioni diverse da effettuare.

» **Ad esempio**: Eliminare i messaggi rilevati dal filtro SpamRazer, ma non eliminare i messaggi contrassegnati come spam dal filtro Block list e-mail.

6.2.1 Configurazione operazioni spam

Nella scheda **Azioni**, selezionare un'opzione che definisce l'azione da intraprendere sui messaggi contrassegnati come spam.


Generale
Eccezioni
Azioni
Selezionare l'azione da eseguire quando questo filtro blocca un messaggio di spam
Azioni
E-mail in quarantena
Elimina e-mail
Effettuare le azioni indicate di seguito
Consegnare messaggio di posta elettronica alla cassetta postale:
Nella posta in arrivo
Nella cartella secondaria della cassetta postale di Exchange
Inbox/New Senders
Inviare all'indirizzo di posta elettronica:
Administrator@domaina.tcv
Sposta nella cartella su disco:
Contrassegna il messaggio con un testo specifico:
NEWSENDER
Specificare in che modo applicare l'etichetta al messaggio di posta elettronica:
Anteponi all'oggetto
Accoda motivo di blocco all'oggetto del messaggio di posta elettronica
Opzioni di registrazione
Registra occorrenza regola nel seguente file
C:\Program Files (x86)\GFI\MailEssentials\Antispam\logs\newsenders.log

Schermata 84: operazioni antispam

Azione	Descrizione
E-mail in quarantena	I messaggi rilevati come spam verranno archiviati in Quarantine Store. Se il messaggio è inserito nella quarantena, tutte le altre operazioni antispam saranno disabilitate. Per ulteriori informazioni, fare riferimento a Quarantena (pagina 203).
Elimina e-mail	Eliminare un messaggio bloccato da quel particolare filtro antispam. Se il messaggio viene eliminato, tutte le altre operazioni antispam saranno disabilitate.

Azione	Descrizione
Consegnare messaggio di posta elettronica alla cassetta postale	Scegliere la cartella dove recapitare la posta. Le opzioni disponibili sono: » **Nella posta in arrivo**: inoltra lo spam nella posta in arrivo dell'utente. » **Nella cartella posta indesiderata di Exchange**: inoltra lo spam nella cartella posta indesiderata predefinita dell'utente. Questa opzione funziona solo quando GFI MailEssentials è installato su Microsoft Exchange. Non è disponibile per il filtro Nuovi mittenti. » **Nella cartella secondaria della cassetta postale di Exchange**: inoltra tutto lo spam a una cartella specifica della cassetta postale dell'utente. Digitare la cartella dove spostare i messaggi spam. • **Esempio 1:** digitare `Spam sospetto` per una cartella personalizzata da creare allo stesso livello della cartella Posta in arrivo. • **Esempio 2:** digitare `Posta in arrivo/Spam sospetto` per una cartella personalizzata da creare nella cartella Posta in arrivo. **NOTA:** Questa opzione richiede che: • GFI MailEssentials sia installato in un computer Microsoft® Exchange Server. Se GFI MailEssentials non è installato in un computer Microsoft® Exchange Server, configurare il server di posta per l'inoltro dei messaggi tramite Gestione regole. Per ulteriori informazioni, fare riferimento a Spostamento messaggi spam nelle cartelle della cassetta postale degli utenti (pagina 263). • Il server di posta è Microsoft® Exchange Server 2003 o Microsoft® Exchange Server 2007/2010 con il ruolo Server cassetta postale. L'abilitazione di questa opzione su Microsoft® Exchange 2010 richiede un utente dedicato. Per ulteriori informazioni, fare riferimento a Spostamento spam nella cartella di Exchange 2010 (pagina 266).
Inviare all'indirizzo di posta elettronica	Invia la posta identificata come spam a un indirizzo e-mail specifico. **Esempio:** Inoltra tutto lo spam a un indirizzo e-mail controllato da qualcuno che controlla la posta che potrebbe essere stata erroneamente contrassegnata come spam. L'oggetto del messaggio sarà nel formato: `[destinatario] [oggetto]`
Sposta nella cartella su disco	Salva il messaggio rilevato come spam nel percorso indicato, **Esempio:** `C:\Spam\` I nomi file dei messaggi salvati sono nel formato seguente: `[Mittente_destinatario_oggetto_numero_.eml]` **Esempio:** `C:\Spam\jim@comp.com_bob@comp.com_MailOffers_1_.eml`)
Contrassegna il messaggio con un testo specifico	Selezionare questa opzione per aggiungere un contrassegno all'oggetto del messaggio. Digitare il testo da usare per il contrassegno e indicare dove posizionare il tag: » **Anteponi all'oggetto**: inserisce il tag specificato all'inizio (ad es. come prefisso) del testo oggetto del messaggio. **Esempio:** `[SPAM]Web Mail gratuita` » **Accoda all'oggetto**: inserisce il tag specificato alla fine (ad es. come suffisso) del testo oggetto del messaggio. **Esempio:** `Web Mail gratuita[SPAM]` » **Aggiungi etichetta in un'intestazione X...**: aggiunge il tag specificato come nuova intestazione X del messaggio. In questo caso, l'intestazione X avrà il seguente formato: • X-GFIME-SPAM: [TESTO TAG] • X-GFIME-SPAM-REASON: [MOTIVO] **Esempio:** – X-GFIME-SPAM: [Messaggio spam] – X-GFIME-SPAM-REASON: [Controllo block list DNS IP non riuscito - Inviato da dominio inserito nella block list] **NOTA** Gestione regole può essere utilizzata per spostare i messaggi quando si utilizza questa funzione.

Azione	Descrizione
Accoda motivo di blocco all'oggetto del messaggio di posta elettronica	Se è abilitata questa opzione, il nome del filtro che ha bloccato la posta e il motivo del blocco vengono aggiunti all'oggetto del messaggio bloccato.
Registra occorrenza regola nel seguente file	Registra l'occorrenza del messaggio spam in un file di registro a scelta dell'utente. Per impostazione predefinita, i file di registro vengono archiviati in: *<GFI MailEssentials percorso di installazione>*\GFI\MailEssentials\AntiSpam\Logs\<nomefiltro>.log **NOTA** I file di registro potrebbero diventare molto grandi. GFI MailEssentials consente la rotazione del registro, durante la quale i nuovi file di registro vengono creati periodicamente oppure quando il file del registro raggiunge una determinata dimensione. Per abilitare la rotazione del file di registro, selezionare **Antispam > Impostazioni antispam**. Selezionare la scheda **Registrazione messaggi antispam**, quindi selezionare **Abilita rotazione file di registro**. Indicare la condizione di rotazione: in base al tempo o alle dimensioni file.

6.3 Ordinamento filtri antispam in base alla priorità.

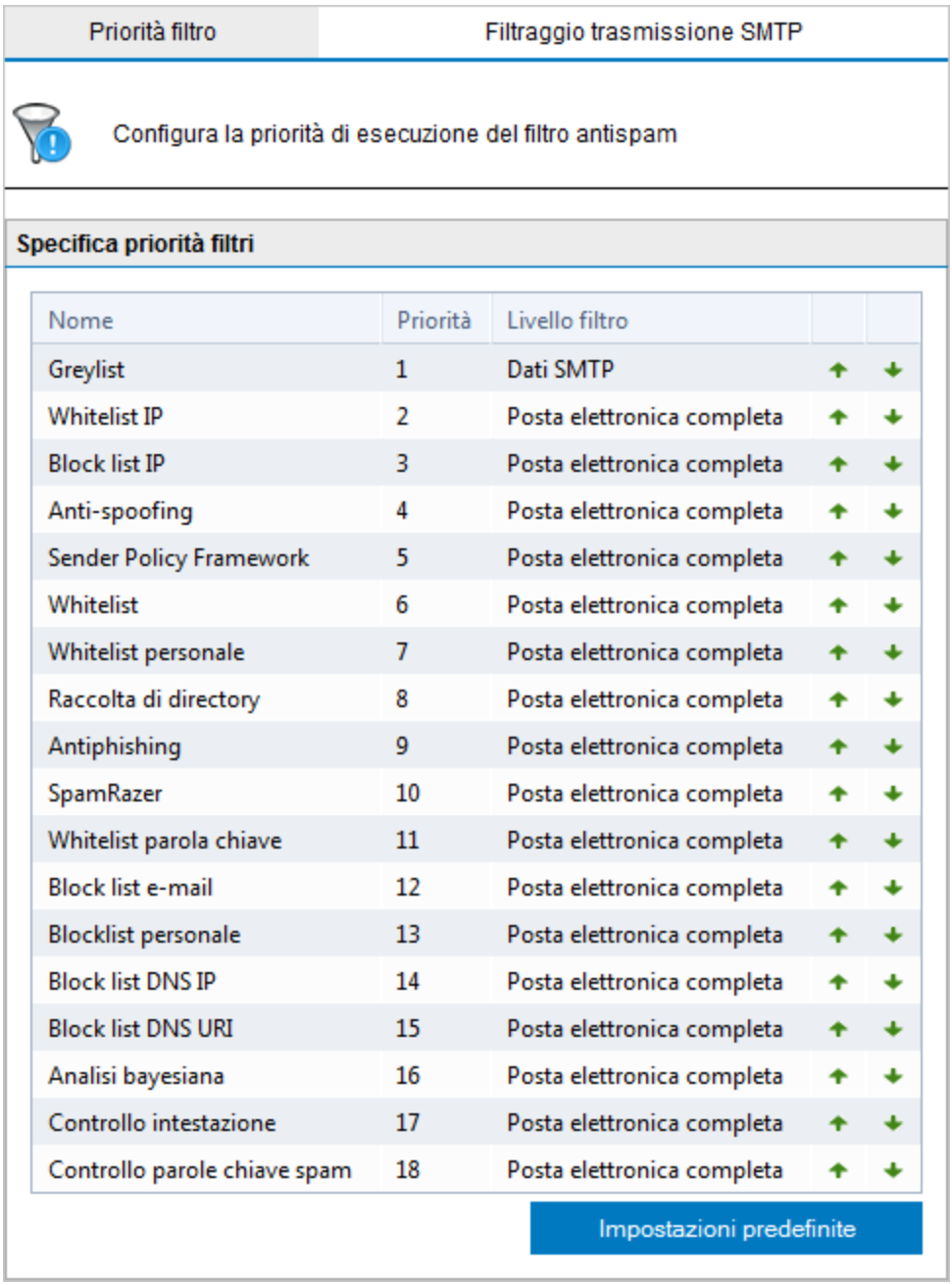
In GFI MailEssentials, è possibile personalizzare l'ordine di applicazione dei controlli antispam ai messaggi in arrivo.

NOTA

L'ordine dei filtri disponibili può essere personalizzato, ad eccezione del filtro **Nuovi mittenti**, che viene sempre impostato sulla priorità più bassa. Questo è dovuto alla dipendenza dai risultati dei controlli whitelist e di altri filtri antispam.

La priorità predefinita è consigliata nella maggioranza delle situazioni.

1. Fare clic su **Antispam > Priorità filtro**.


Priorità filtro
Filtraggio trasmissione SMTP
Configura la priorità di esecuzione del filtro antispam
Specifica priorità filtri
Nome
Priorità
Livello filtro
Greylist 1 Dati SMTP
Whitelist IP 2 Posta elettronica completa
Block list IP 3 Posta elettronica completa
Anti-spoofing 4 Posta elettronica completa
Sender Policy Framework 5 Posta elettronica completa
Whitelist 6 Posta elettronica completa
Whitelist personale 7 Posta elettronica completa
Raccolta di directory 8 Posta elettronica completa
Antiphishing 9 Posta elettronica completa
SpamRazer 10 Posta elettronica completa
Whitelist parola chiave 11 Posta elettronica completa
Block list e-mail 12 Posta elettronica completa
Blocklist personale 13 Posta elettronica completa
Block list DNS IP 14 Posta elettronica completa
Block list DNS URI 15 Posta elettronica completa
Analisi bayesiana 16 Posta elettronica completa
Controllo intestazione 17 Posta elettronica completa
Controllo parole chiave spam 18 Posta elettronica completa
Impostazioni predefinite

Schermata 85: assegnazione priorità filtro

2. Selezionare un filtro e fare clic sul pulsante ↑ (su) per assegnare una priorità superiore o fare clic sul pulsante ↓ (giù) per impostarne una inferiore.

> **NOTA**
> Per ripristinare l'ordine predefinito dei filtri, fare clic su **Impostazioni predefinite**.

3. Fare clic su **Applica**.

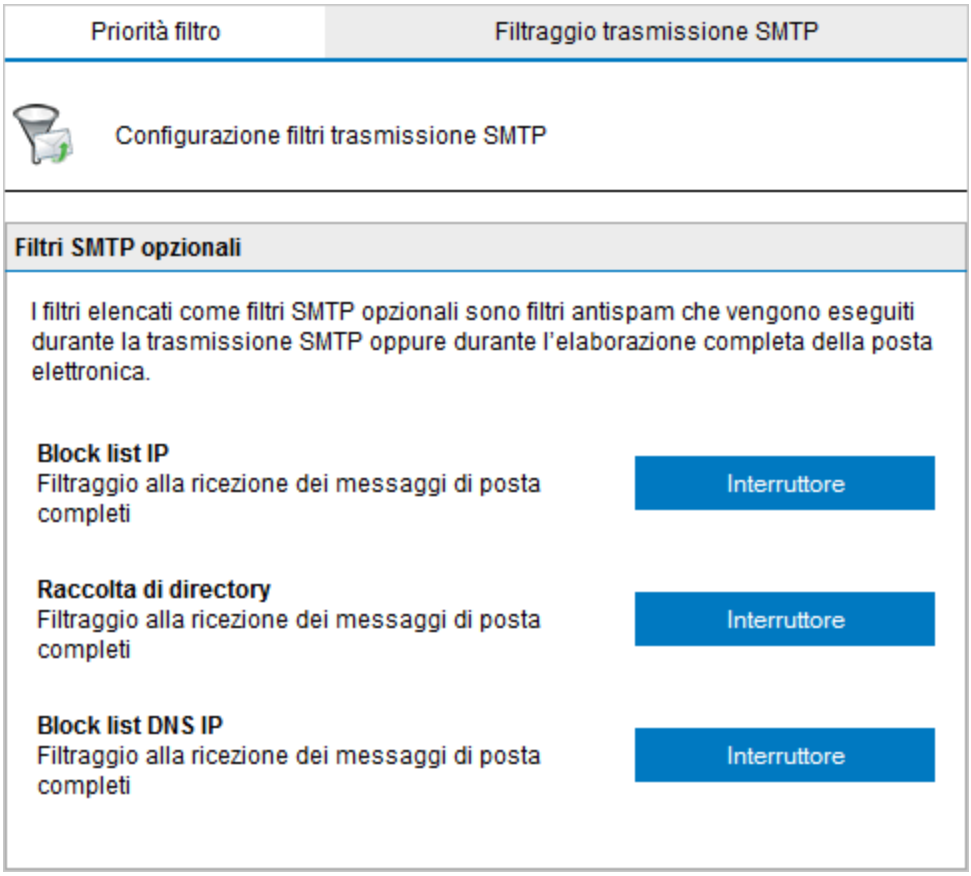
6.4 Filtraggio trasmissione SMTP

In GFI MailEssentials, alcuni filtri antispam possono essere configurati per essere eseguiti al ricevimento del messaggio completo o a livello SMTP o al livello di trasmissione SMTP. Nel filtro trasmissione SMTP, i messaggi di posta elettronica vengono scansionati mentre vengono ricevuti.

Il filtro a livello SMTP interrompe la connessione della posta e dunque arresta il download dell'intero messaggio, risparmiando la larghezza di banda e le risorse di elaborazione. In questo caso, la connessione viene interrotta immediatamente e i messaggi non devono superare nessun altro filtro antispam.

IMPORTANTE
Per ottenere il meglio dal filtro trasmissione SMTP, utilizzarlo quando GFI MailEssentials è installato in un gateway Internet o quando è il primo server a ricevere le e-mail da Internet.

1. Accedere a **Antispam** > **Priorità filtro** e selezionare la scheda **Filtraggio trasmissione SMTP**.


Priorità filtro
Filtraggio trasmissione SMTP
Configurazione filtri trasmissione SMTP
Filtri SMTP opzionali
I filtri elencati come filtri SMTP opzionali sono filtri antispam che vengono eseguiti durante la trasmissione SMTP oppure durante l'elaborazione completa della posta elettronica.
Block list IP
Filtraggio alla ricezione dei messaggi di posta completi
Interruttore
Raccolta di directory
Filtraggio alla ricezione dei messaggi di posta completi
Interruttore
Block list DNS IP
Filtraggio alla ricezione dei messaggi di posta completi
Interruttore

Schermata 86: proprietà di Filtraggio trasmissione SMTP

2. Fare clic su **Cambia** per attivare o disattivare il filtro di Raccolta di directory scegliendo tra:

Opzione	Descrizione
Filtraggio alla ricezione dei messaggi di posta completi	Il filtraggio viene effettuato alla ricezione dell'intero messaggio.
Filtraggio durante trasmissione SMTP	Il filtraggio avviene durante la trasmissione SMTP. Se viene selezionata questa opzione, il filtro verrà sempre eseguito prima degli altri filtri antispam.

NOTA
Il filtro Greylist viene eseguito solo a livello di trasmissione SMTP.

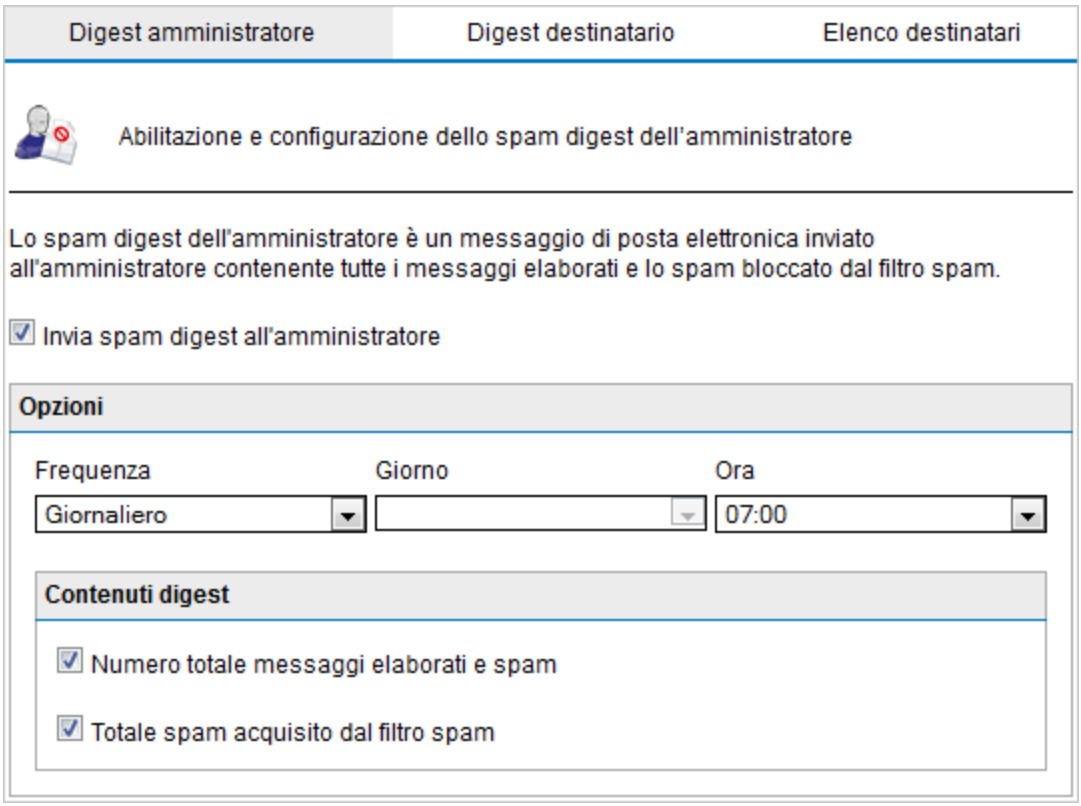
3. Fare clic su **Applica**.

6.5 Spam Digest

Lo Spam Digest è un breve rapporto inviato a un amministratore o a un utente tramite posta elettronica. Questo rapporto elenca il numero totale di messaggi elaborati da GFI MailEssentials e il numero di messaggi spam bloccati in un periodo specifico di tempo (dall'ultimo spam digest).

6.5.1 Configurazione spam digest - Spam digest amministratore

1. Fare clic su **Antispam > Spam Digest**.


Digest amministratore
Digest destinatario
Elenco destinatari
Abilitazione e configurazione dello spam digest dell'amministratore
Lo spam digest dell'amministratore è un messaggio di posta elettronica inviato all'amministratore contenente tutte i messaggi elaborati e lo spam bloccato dal filtro spam.
Invia spam digest all'amministratore
Opzioni
Frequenza
Giorno
Ora
Giornaliero
07:00
Contenuti digest
Numero totale messaggi elaborati e spam
Totale spam acquisito dal filtro spam

Schermata 87: proprietà spam digest/spam digest amministratore

2. Dalla scheda **Digest amministratore**, fare clic su **Invia spam digest all'amministratore** per abilitare lo spam digest.

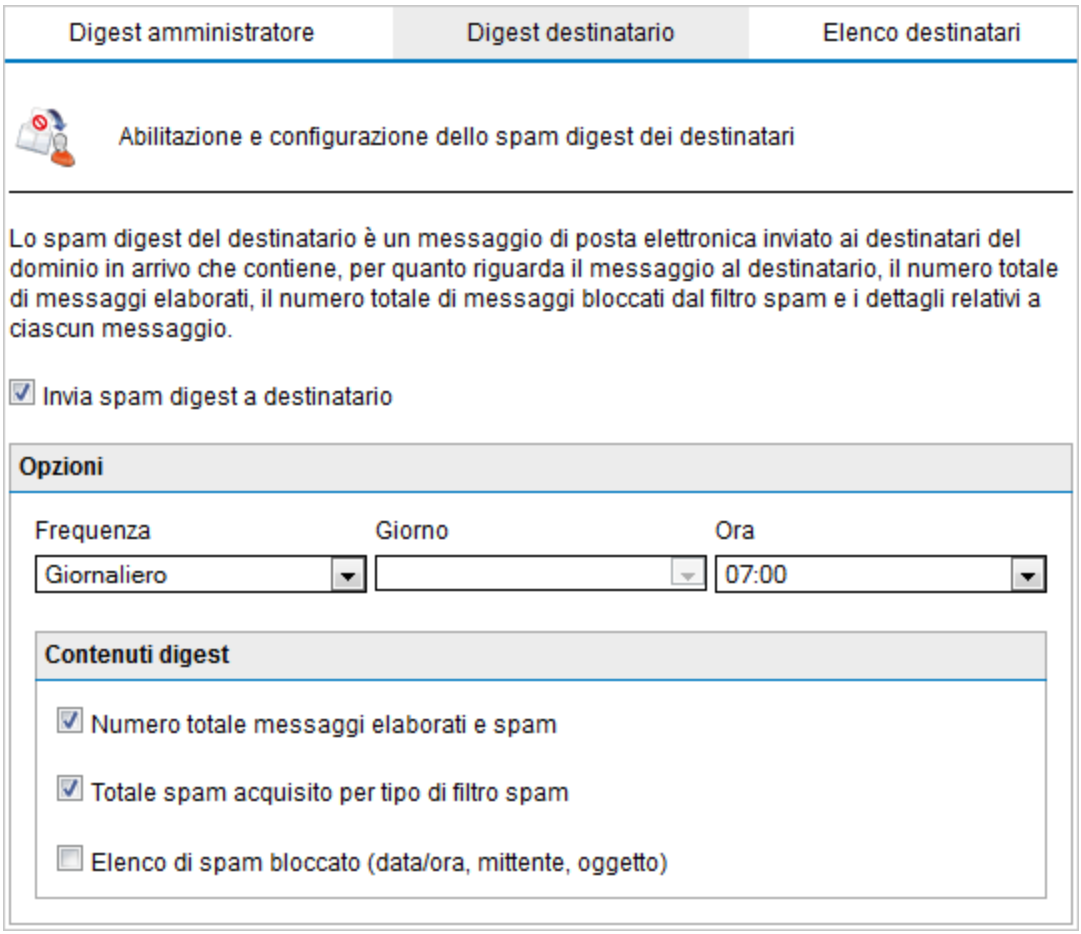
3. Configurare la frequenza di invio desiderata (giornaliera, settimanale, mensile) e indicare una data e un periodo per l'invio del messaggio di posta elettronica.

4. Indicare il contenuto del digest che verrà inviato nel messaggio di posta elettronica, selezionando **Numero totale messaggi elaborati e spam** o **Totale spam acquisito dal filtro spam** o entrambi.

5. Finalizzare le impostazioni facendo clic su **Applica**.

6.5.2 Configurazione spam digest - Spam digest destinatario

1. Fare clic su **Antispam > Spam Digest**.


Digest amministratore
Digest destinatario
Elenco destinatari
Abilitazione e configurazione dello spam digest dei destinatari
Lo spam digest del destinatario è un messaggio di posta elettronica inviato ai destinatari del dominio in arrivo che contiene, per quanto riguarda il messaggio al destinatario, il numero totale di messaggi elaborati, il numero totale di messaggi bloccati dal filtro spam e i dettagli relativi a ciascun messaggio.
Invia spam digest a destinatario
Opzioni
Frequenza
Giorno
Ora
Giornaliero
07:00
Contenuti digest
Numero totale messaggi elaborati e spam
Totale spam acquisito per tipo di filtro spam
Elenco di spam bloccato (data/ora, mittente, oggetto)

Schermata 88: spam digest destinatario

2. Dalla scheda **Digest destinatario**, fare clic su **Invia spam digest a destinatario** per abilitare lo spam digest.

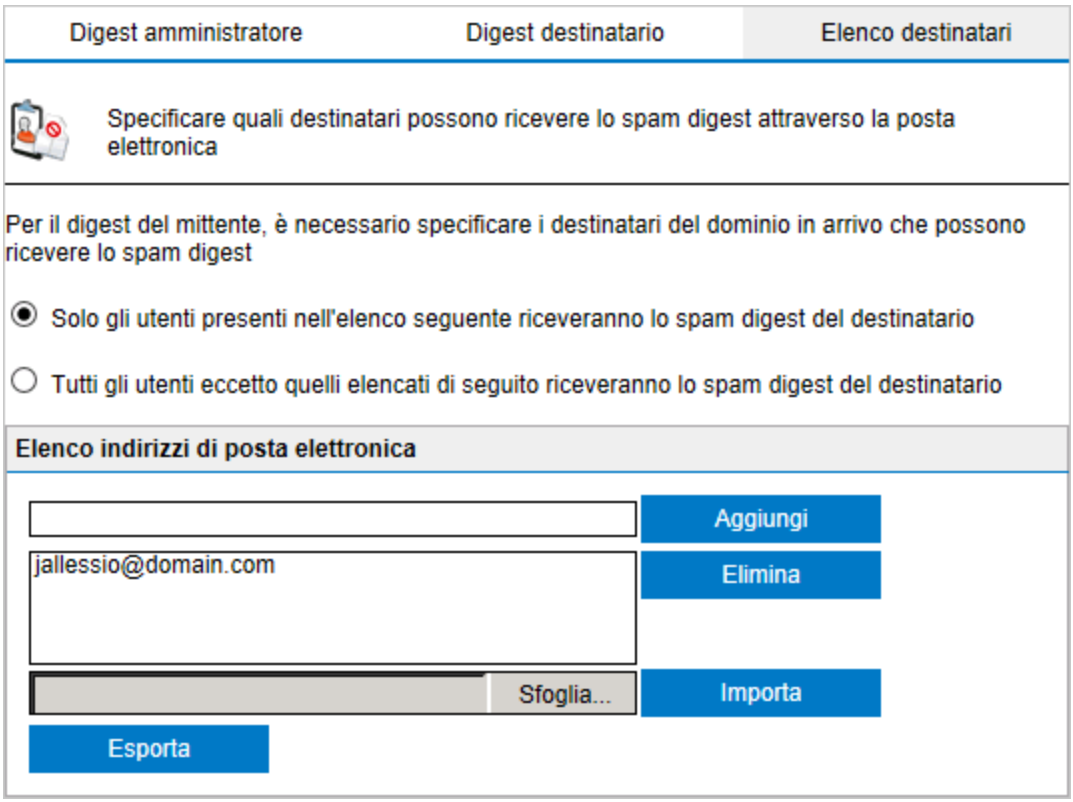
3. Configurare la frequenza di invio desiderata (giornaliera, settimanale, mensile) e indicare una data e un periodo per l'invio del messaggio di posta elettronica.

4. Specificare il contenuto del digest che verrà inviato nel messaggio di posta elettronica:

» Numero totale messaggi elaborati e spam

» Totale spam acquisito per tipo di filtro spam

» Elenco dello spam bloccato o di eventuali combinazioni di opzioni necessarie.


Digest amministratore
Digest destinatario
Elenco destinatari
Specificare quali destinatari possono ricevere lo spam digest attraverso la posta elettronica
Per il digest del mittente, è necessario specificare i destinatari del dominio in arrivo che possono ricevere lo spam digest
Solo gli utenti presenti nell'elenco seguente riceveranno lo spam digest del destinatario
Tutti gli utenti eccetto quelli elencati di seguito riceveranno lo spam digest del destinatario
Elenco indirizzi di posta elettronica
Aggiungi
jallessio@domain.com
Elimina
Sfoglia...
Importa
Esporta

Schermata 89: elenco destinatari spam digest

4. Fare clic sulla scheda **Elenco destinatari**, aggiungere gli utenti che riceveranno lo spam digest e selezionare il metodo utilizzato per determinare chi lo dovrà ricevere.

Le opzioni disponibili sono:

» Solo gli utenti presenti nell'elenco seguente riceveranno lo spam digest del destinatario.

» Tutti gli utenti eccetto quelli elencati di seguito riceveranno lo spam digest del destinatario.

> **NOTA**
> È possibile importare l'elenco richiesto di utenti anche da un file in formato XML con la medesima struttura utilizzata da GFI MailEssentials per l'esportazione dei file.

6. Per finalizzare le impostazioni, fare clic su **Applica**.

6.6 Impostazioni antispam

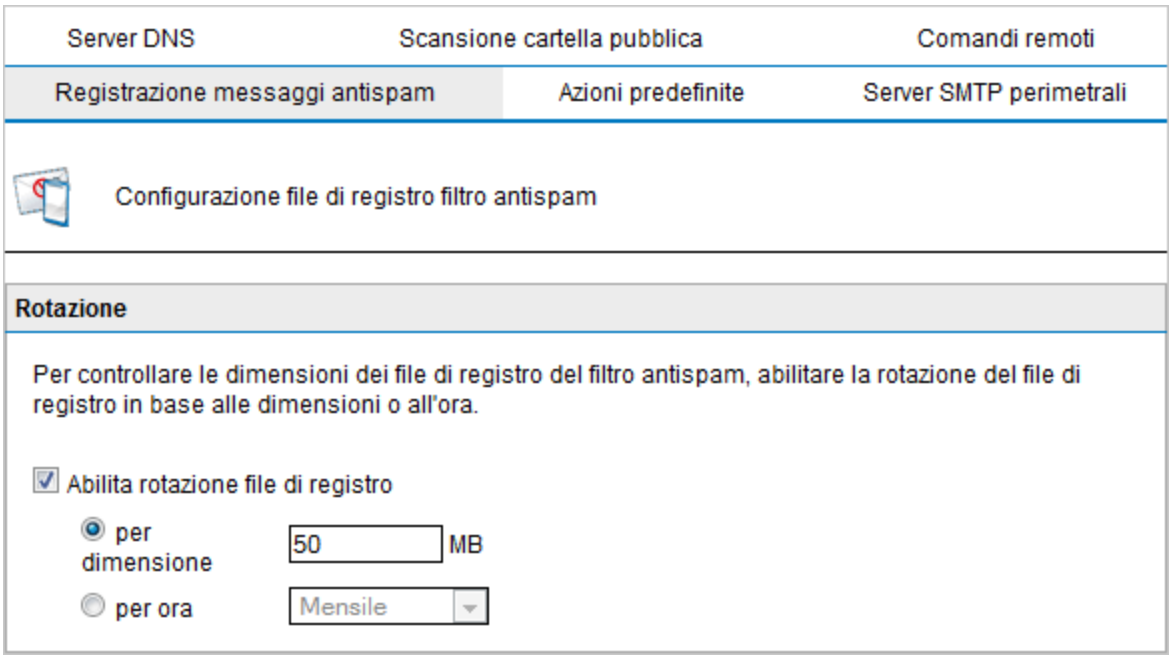
Le seguenti impostazioni sono configurabili esclusivamente per i filtri antispam e per i messaggi di posta bloccati da essi.

6.6.1 Rotazione file di registro

Con il corso del tempo, i file di registro potrebbero diventare molto grandi. GFI MailEssentials consente la rotazione del registro, durante la quale i nuovi file di registro vengono creati periodicamente oppure quando il file del registro raggiunge una determinata dimensione.

Per abilitare la rotazione file di registro:

1. Fare clic su **Antispam > Impostazioni antispam**.



Schermata 90: Rotazione file di registro

2. Dalla scheda **Registrazione messaggi antispam**, fare clic su **Abilita rotazione file di registro** e indicare la condizione di rotazione (**per dimensione** o **per ora**).

3. Fornire i valori di dimensioni o di tempo e fare clic su **Applica**.

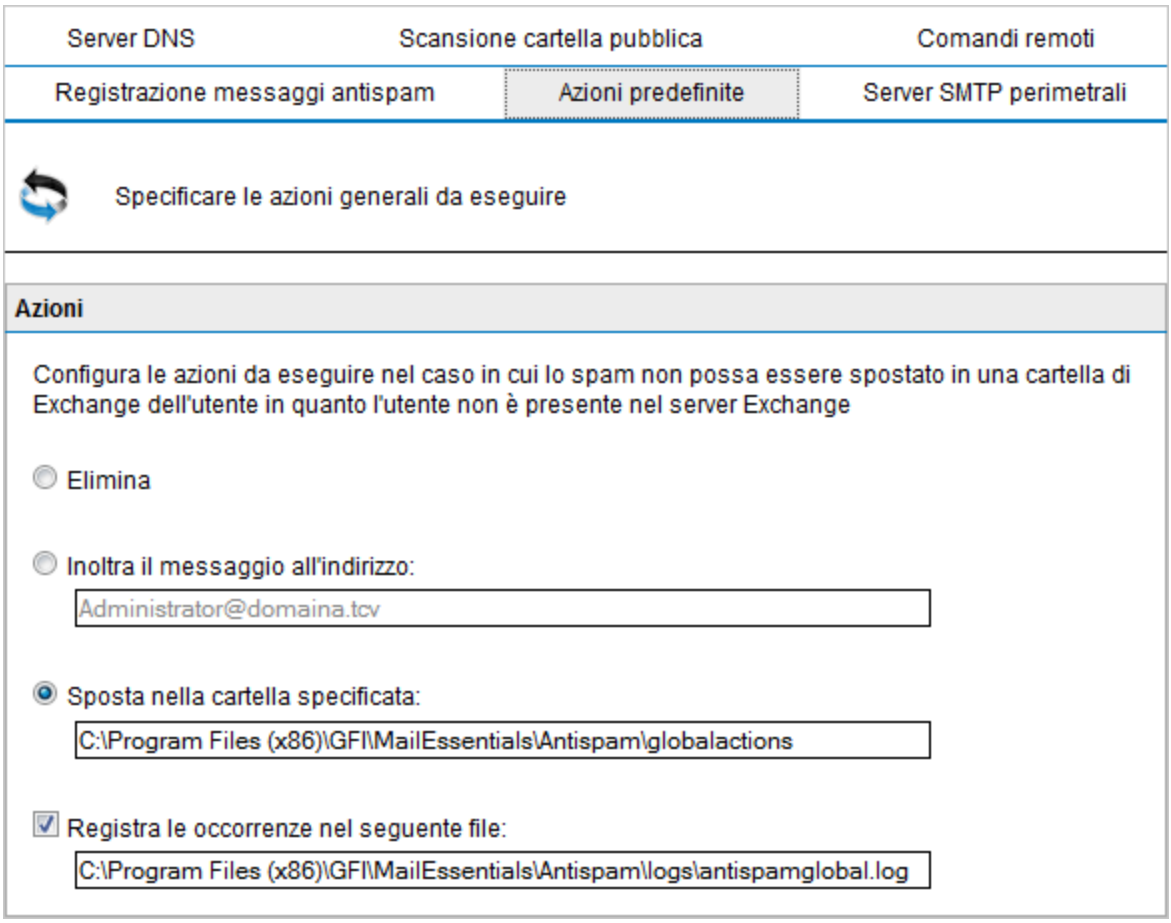
6.6.2 Operazioni antispam predefinite

Una grande quantità di spam viene inviata a indirizzi di posta elettronica che non esistono più. Normalmente, questi messaggi vengono semplicemente eliminati. Tuttavia, a scopo di valutazione o di risoluzione problemi, è possibile spostarli in una cartella o inoltrarli a un indirizzo di posta elettronica specifico.

> **NOTA**
> Questa sezione si applica solo alle installazioni su Microsoft® Exchange Server dove è abilitata l'azione antispam **Spostare il messaggio nella sottocartella della cassetta postale dell'utente**. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148).
> Sugli altri server di posta, la scheda azioni predefinite antispam non viene visualizzata.

Configurazione operazioni antispam predefinite

1. Fare clic su **Antispam > Impostazioni antispam**.


Server DNS
Scansione cartella pubblica
Comandi remoti
Registrazione messaggi antispam
Azioni predefinite
Server SMTP perimetrali
Specificare le azioni generali da eseguire
Azioni
Configura le azioni da eseguire nel caso in cui lo spam non possa essere spostato in una cartella di Exchange dell'utente in quanto l'utente non è presente nel server Exchange
Elimina
Inoltra il messaggio all'indirizzo:
Administrator@domaina.tcv
Sposta nella cartella specificata:
C:\Program Files (x86)\GFI\MailEssentials\Antispam\globalactions
Registra le occorrenze nel seguente file:
C:\Program Files (x86)\GFI\MailEssentials\Antispam\logs\antispamglobal.log

Schermata 91: azioni predefinite

2. Selezionare **Azioni predefinite** e scegliere tra:

» Eliminare il messaggio.

» Inoltrarlo a un indirizzo di posta elettronica.

» Spostarlo in una cartella specifica.

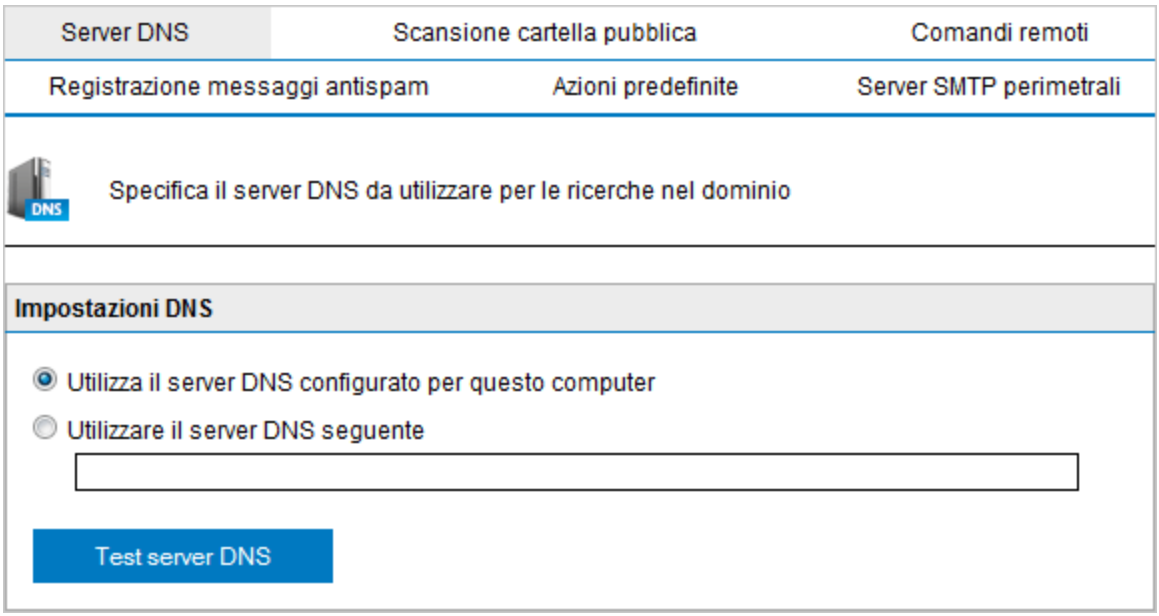
3. Per registrare le occorrenze in un file di registro, selezionare **Registra occorrenze nel seguente file**.

4. Fare clic su **Applica**.

6.6.3 Impostazioni server DNS

Le impostazioni del server DNS sono molto importanti in GFI MailEssentials, poiché una serie di filtri antispam, tra cui la block list DNS IP, la block list DNS URI e SpamRazer eseguono la ricerca del dominio durante il filtraggio dello spam.

1. Da GFI MailEssentials Configuration, fare clic su **Antispam > Impostazioni antispam**.


Server DNS
Scansione cartella pubblica
Comandi remoti
Registrazione messaggi antispam
Azioni predefinite
Server SMTP perimetrali
Specifica il server DNS da utilizzare per le ricerche nel dominio
Impostazioni DNS
Utilizza il server DNS configurato per questo computer
Utilizzare il server DNS seguente
Test server DNS

Schermata 92: impostazioni server DNS

1. Dalla scheda **Server DNS**, selezionare:

Opzione	Descrizione
Utilizza il server DNS configurato per questo computer	Selezionare questa opzione per utilizzare lo stesso server DNS utilizzato dal sistema operativo dove è installato GFI MailEssentials.
Utilizzare il server DNS seguente	Selezionare questa opzione per specificare un server DNS diverso da quello utilizzato dal computer locale.

2. Fare clic su **Test server DNS** per provare la connettività con il server DNS specificato. Se la verifica ha esito negativo, specificare un altro server DNS.

3. Fare clic su **Applica**.

6.6.4 Comandi remoti

I comandi remoti facilitano l'aggiunta di domini o indirizzi di posta elettronica alla block list e-mail/whitelist, oltre ad aggiornare il filtro bayesiano con spam o ham (messaggi validi).

I comandi remoti funzionano tramite l'invio di un messaggio a GFI MailEssentials. Indirizzando un messaggio di posta a **rcommands@mailessentials.com** (configurabile a piacere), GFI MailEssentials riconoscerà il messaggio come contenente comandi e processi remoti come quelli descritti di seguito.

Con i comandi remoti, è possibile eseguire le seguenti attività:

1. Aggiungere spam o ham al database di analisi bayesiana.

2. Aggiungere le parole chiave alla funzione di controllo parole chiave nell'oggetto o di controllo parole chiave nel corpo.

3. Aggiungere gli indirizzi di posta al filtro blocklist e-mail e whitelist.

Configurazione comandi remoti

1. Fare clic su **Antispam > Impostazioni antispam**, selezionare la scheda **Comandi remoti** e quindi su **Abilita comandi remoti**.

2. Modificare l'indirizzo di posta elettronica a cui devono essere inviati i comandi remoti.

NOTA
L'indirizzo di posta elettronica **NON** deve essere un dominio locale. L'indirizzo di posta elettronica predefinito è **rcommands@mailessentials.com**. Una cassetta postale per l'indirizzo configurato non deve esistere necessariamente, ma la parte dominio dell'indirizzo deve essere costituita da un dominio dell'indirizzo di posta elettronica reale che restituisce un risultato positivo a una ricerca di un record MX tramite DNS. Può essere anche un account di posta elettronica pubblico che è possibile gestire (ad esempio gmail o yahoo mail).

3. In alternativa, configurare una protezione di base per i comandi remoti:

» Una password condivisa da includere nel messaggio di posta. Per ulteriori informazioni, fare riferimento a Utilizzo dei comandi remoti (pagina 160).

» Quali utenti sono autorizzati a inviare messaggi di posta con comandi remoti.

4. Fare clic su **Applica**.

Utilizzo dei comandi remoti

I comandi remoti possono essere inviati per posta a GFI MailEssentials da un client di posta elettronica all'interno del dominio. Condizioni per l'invio di comandi remoti:

» il messaggio di posta elettronica deve essere in formato testo normale

» l'oggetto del messaggio viene ignorato

» Per tutti i comandi deve essere utilizzata la seguente sintassi:

```
<nome comando>: <parametro1>, <parametro2>, <parametro3>, … ;
```

Ad esempio:`ADDBLIST: spammer@spam.com;`

» Nel corpo del messaggio di posta elettronica può essere presente più di un comando, ciascuno deve essere separato da un punto e virgola (;).

» Se una password è configurata per i comandi remoti, immetterla nella prima riga mediante la sintassi seguente:

```
PASSWORD: <password condivisa>;
```

» I nomi dei comandi applicano la distinzione tra maiuscole e minuscole e devono essere scritti solo in MAIUSCOLO.

» Non sono supportate condizioni come `IF, AND, OR`.

» I comandi remoti possono essere utilizzati solo per aggiungere voci e non per modificare o eliminare quelle esistenti.

Comandi parola chiave

Utilizzare i comandi parola chiave per aggiungere parole chiave o combinazioni delle stesse negli elenchi corpo o oggetto del filtro Controllo parola chiave.

I comandi disponibili:

» ADDSUBJECT: aggiunge le parole chiave specificate al database di controllo parole chiave nell'oggetto.

- Esempio: ADDSUBJECT: sex, porn, spam;

» ADDBODY: aggiunge le parole chiave specificate al database di controllo parole chiave nel corpo.

- Esempio: ADDBODY: gratis, “totalmente gratis”, “assolutamente gratis”;

> **NOTA**
> Quando si configurano frasi diverse dalle parole singole, racchiuderle tra virgolette doppie (“ ”).

Comandi block list

Utilizzare i comandi block list per aggiungere un indirizzo di posta elettronica singolo o un intero dominio alla block list della posta elettronica.

I comandi disponibili:

» `ADDBLIST: <e-mail>;`

- Esempio: `ADDBLIST: user@somewhere.com;`

> **NOTE**
> 1. Aggiunge un intero dominio alla block list anteponendo un carattere jolly al nome del dominio.
>
> **Esempio:** `ADDBLIST: *@domain.com;`
>
> 2. I caratteri jolly non possono essere utilizzati nei nomi di dominio.
>
> **Ad esempio:**`ADDBLIST: *@*.domain.com;` non è valido e verrà rifiutato.
>
> 3. Per motivi di sicurezza, può esserci solo un comando `ADDBLIST` in un messaggio di posta e solo un indirizzo può essere indicato come parametro del comando. Il parametro è l’indirizzo di posta di un utente o un dominio:
>
> **Esempio:**`ADDBLIST: spammer@spam.com;` o `ADDBLIST:*@spammers.org;`

Comandi del filtro bayesiano

Aggiungere messaggi spam o posta valida (ham) al database del filtro bayesiano. I comandi disponibili:

Elenco	Descrizione
ADDASSPAM	Indica al filtro bayesiano di classificare la posta come spam.
ADDASGOODMAIL	Indica al filtro bayesiano di classificare la posta come HAM.

> **NOTA**
> Questi comando non hanno parametri, il contenuto del messaggio stesso è il parametro.

Registrazione comandi remoti

Per tenere traccia delle modifiche effettuate al database di configurazione mediante i comandi remoti, ciascun messaggio contenente gli stessi (persino se il messaggio con i comandi remoti era non valido) viene salvato in:

<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\AntiSpam\ADBRProcessed\

Il nome file di ciascun messaggio viene formattato in base al seguente formato:

» `<indirizzo_email_mittente>_SUCCESS_<timestamp>.eml`: qualora l'elaborazione venga completata correttamente.

» `<indirizzo_email_mittente>_FAILED_<timestamp>.eml`: qualora l'elaborazione non venga completata.

> **NOTA**
> Timestamp viene formattato come `aaaammgghhmmss`.

6.7 SpamTag per Microsoft Outlook

Il plugin GFI MailEssentials SpamTag è un componente aggiuntivo per Microsoft Outlook che installa una barra degli strumenti nei computer degli utenti finali, offrendo così un certo controllo agli utenti nella gestione dei messaggi di spam. Il plugin sincronizza inoltre le impostazioni di Posta indesiderata di Microsoft Outlook con GFI MailEssentials.

Mentre la funzionalità di Microsoft Outlook consente agli utenti di gestire i messaggi spam dal lato cliente, con il plugin di SpamTag gli utenti possono gestirli a livello di server.

L'amministratore di GFI MailEssentials può scegliere quali delle seguenti funzioni e caratteristiche desidera abilitare:

» Addestra il filtro analisi bayesiana

» Aggiunta di mittenti e/o domini alla block list personale o alla whitelist personale

» Sincronizzazione automatica di mittenti consentiti e bloccati di Microsoft Outlook all'interno della Whitelist e Block list personale di GFI MailEssentials, rispettivamente.

» Aggiunta automatica dei contatti degli utenti nella Whitelist personale.

> **NOTA**
> Gli utenti a cui è assegnato accesso completo a GFI MailEssentials sono inoltre autorizzati ad aggiungere mittenti/domini alla Block list globale e Whitelist globale di e-mail di GFI MailEssentials.

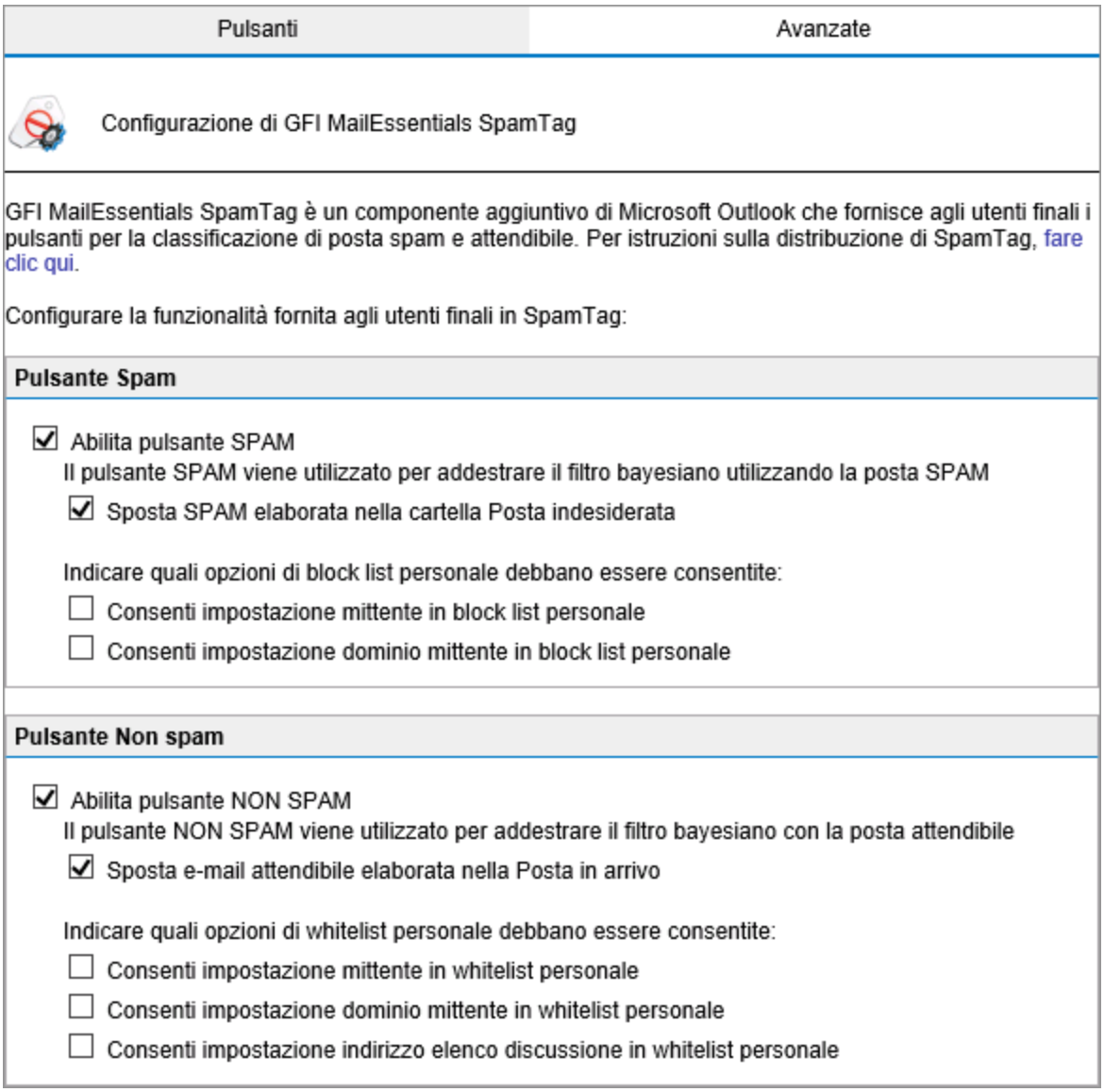
> **NOTA**
> Quando si utilizza SpamTag, installare Windows Communication Foundation HTTP Activation sul server GFI MailEssentials. Per eseguire questa operazione, selezionare **Server Manager > Funzionalità > Aggiungi funzionalità > .NET Framework > Attivazione di WCF > Attivazione HTTP**.

6.7.1 Scelta funzioni SpamTag

L'amministratore di GFI MailEssentials può configurare le funzioni di SpamTag da rendere disponibili agli utenti. Ad esempio, può consentire agli utenti di aggiungere mittenti alla whitelist personale ma disabilitare l'aggiunta di domini alla whitelist personale. SpamTag può anche essere configurato per sostituire le funzionalità di posta indesiderata di Microsoft Outlook.

Per configurare le funzioni di SpamTag:

1. Fare clic su **Antispam > SpamTag**.


Pulsanti
Avanzate
Configurazione di GFI MailEssentials SpamTag
GFI MailEssentials SpamTag è un componente aggiuntivo di Microsoft Outlook che fornisce agli utenti finali i pulsanti per la classificazione di posta spam e attendibile. Per istruzioni sulla distribuzione di SpamTag, fare clic qui.
Configurare la funzionalità fornita agli utenti finali in SpamTag:
Pulsante Spam
Abilita pulsante SPAM
Il pulsante SPAM viene utilizzato per addestrare il filtro bayesiano utilizzando la posta SPAM
Sposta SPAM elaborata nella cartella Posta indesiderata
Indicare quali opzioni di block list personale debbano essere consentite:
Consenti impostazione mittente in block list personale
Consenti impostazione dominio mittente in block list personale
Pulsante Non spam
Abilita pulsante NON SPAM
Il pulsante NON SPAM viene utilizzato per addestrare il filtro bayesiano con la posta attendibile
Sposta e-mail attendibile elaborata nella Posta in arrivo
Indicare quali opzioni di whitelist personale debbano essere consentite:
Consenti impostazione mittente in whitelist personale
Consenti impostazione dominio mittente in whitelist personale
Consenti impostazione indirizzo elenco discussione in whitelist personale

2. Dall'area **pulsante Spam**, configurare le funzioni relative a falsi negativi, ovvero quei casi in cui i messaggi di spam non vengono rilevati come tali:

Opzione	Descrizione
Abilita pulsante SPAM	Il pulsante **Spam** viene visualizzato in SpamTag e, quando selezionato, il messaggio in questione addestra il filtro analisi bayesiana.
Sposta SPAM elaborata nella cartella Posta indesiderata	Quando si seleziona **Spam**, il messaggio in questione viene automaticamente spostato nella cartella Posta indesiderata di Microsoft Outlook.
Consenti impostazione mittente in block list personale	Sotto il pulsante **Spam** viene visualizzata un'opzione secondaria che consente agli utenti di aggiungere l'indirizzo e-mail del mittente alla loro block list personale. Per poter utilizzare questa opzione, deve essere abilitata Block list personale.
Consenti impostazione dominio mittente in block list personale	Sotto il pulsante **Spam** viene visualizzata un'opzione secondaria che consente agli utenti di aggiungere il dominio del mittente alla loro block list personale. Per poter utilizzare questa opzione, deve essere abilitata Block list personale.

3. Dall'area **pulsante Non spam**, configurare le funzioni relative a falsi positivi, ovvero quei casi in cui i messaggi attendibili vengono erroneamente identificati come spam.:

Opzione	Descrizione
Abilita pulsante NON SPAM	Il pulsante **Non spam** viene visualizzato in SpamTag e, quando selezionato, il messaggio in questione addestra il filtro analisi bayesiana.
Sposta e-mail attendibile elaborata nella Posta in arrivo	Quando si seleziona **Non spam**, il messaggio in questione viene automaticamente spostato nella cartella Posta in arrivo.
Consenti impostazione mittente in whitelist personale	Sotto il pulsante **Non spam** viene visualizzata un'opzione secondaria che consente agli utenti di aggiungere l'indirizzo e-mail del mittente alla loro whitelist personale. Per abilitare questa opzione, deve essere abilitata Whitelist personale.
Consenti impostazione dominio mittente in whitelist personale	Sotto il pulsante **Non spam** viene visualizzata un'opzione secondaria che consente agli utenti di aggiungere il dominio del mittente alla loro whitelist personale. Per abilitare questa opzione, deve essere abilitata Whitelist personale.
Consenti impostazione indirizzo elenco discussione in whitelist personale	Sotto il pulsante **Non spam** viene visualizzata un'opzione secondaria che consente agli utenti di aggiungere newsletter/elenchi di discussione alla loro whitelist. Per abilitare questa opzione, deve essere abilitata Whitelist personale.

4. Dalla scheda **Avanzate** configurare le seguenti opzioni avanzate.

Opzione	Descrizione
Importa impostazioni posta indesiderata di Outlook nella block list personale e nella whitelist personale	Importa gli indirizzi elencati nei Mittenti attendibili e nei Mittenti bloccati di Microsoft Outlook all'interno della Whitelist e Block list personale di GFI MailEssentials. L'elenco di Mittenti attendibili e Mittenti bloccati di Microsoft Outlook è disponibile da **Posta indesiderata > Opzioni posta indesiderata**. **NOTA:** Le importazioni vengono eseguite in automatico in background da SpamTag ogni due ore e l'utente non configura né visualizza alcuna opzione sullo schermo. **NOTA:** Quando l'utente utilizza una versione di Microsoft Outlook installata su un dispositivo alimentato a batteria, come un portatile o tablet, la sincronizzazione automatica non viene eseguita per risparmiare la batteria.
Importa contatti di Outlook nella whitelist personale	Importa l'elenco di contatti di Microsoft Outlook nella Whitelist personale. **NOTA:** Le importazioni vengono eseguite in automatico in background da SpamTag ogni due ore e l'utente non configura né visualizza alcuna opzione sullo schermo. **NOTA:** Quando l'utente utilizza una versione di Microsoft Outlook installata su un dispositivo alimentato a batteria, come un portatile o tablet, la sincronizzazione automatica non viene eseguita per risparmiare la batteria.
Sostituisci Posta indesiderata di Microsoft Outlook	Quando si sceglie questa opzione, le opzioni abilitate in SpamTag sostituiscono quelle equivalenti della Posta indesiderata di Microsoft Outlook, per assicurare che dal lato client sia utilizzato un solo sistema di gestione antispam. Quando gli utenti utilizzano un'opzione di Posta indesiderata di Microsoft Outlook, al suo posto viene eseguita la funzione di SpamTag. Ad esempio, se gli utenti fanno clic su **Non bloccare mai mittente** nella Posta indesiderata di Outlook, al suo posto verrà eseguita la funzione **Non spam** di SpamTag. **NOTA:** Se un'opzione specifica non è abilitata in SpamTag e l'utente utilizza una funzione equivalente in Outlook, non verrà eseguita nessuna azione al momento di selezionare la funzione di Posta indesiderata di Outlook. Ad esempio, se il pulsante Non spam non è abilitato, quando gli utenti selezionano **Non bloccare mai mittente** non verrà eseguita nessuna operazione.
Nascondi il pulsante Console	Nasconde il pulsante Console dalla barra degli strumenti di SpamTag. Non viene fornito nessun accesso diretto alla console di GFI MailEssentials, tuttavia, gli utenti possono sempre accedere digitando manualmente l'URL in un browser. Le impostazioni fornite all'utente nella console di GFI MailEssentials dipendono dalle autorizzazioni Active Directory o da altre Impostazioni Controllo di accesso personalizzate. Per ulteriori informazioni, fare riferimento a Controllo di accesso (pagina 248).

5. Fare clic su **Applica**.

IMPORTANTE

All'avvio di Microsoft Outlook, SpamTag controlla le funzioni abilitate o disabilitate all'interno di GFI MailEssentials. Dopo aver modificato una delle impostazioni di cui sopra, Microsoft Outlook dovrà essere riavviato per l'applicazione delle modifiche.

6.7.2 Requisiti di SpamTag

I computer in cui installare SpamTag devono soddisfare o superare le seguenti specifiche:

Hardware	» Processore – 1 Ghz o superiore » Memoria - Minima 512 MB, 2 GB consigliati » Archiviazione Fisica – 50 MB di archiviazione fisica dedicata per SpamTag
Sistemi operativi supportati	» Windows® 8 & 8.1 » Windows® 7 » Windows® Vista » Windows® XP » Windows® Server 2012 » Windows® Server 2008 » Windows® Server 2003
Versioni supportate di Microsoft Outlook®	» Microsoft Outlook® 2013 » Microsoft Outlook® 2010 » Microsoft Outlook® 2007 » Microsoft Outlook® 2003
Connessione con GFI MailEssentials	SpamTag si connette a GFI MailEssentials sulla porta 80 tramite HTTP. Per confermare la connessione, dal browser del client assicurarsi di poter aprire l'URL di GFI MailEssentials.
Altro software	Microsoft .Net Framework 4: se non disponibile, verrà scaricato e installato automaticamente.

6.7.3 Installazione manuale di SpamTag

Per installare manualmente SpamTag, eseguire il programma di installazione di SpamTag sui computer dei client.

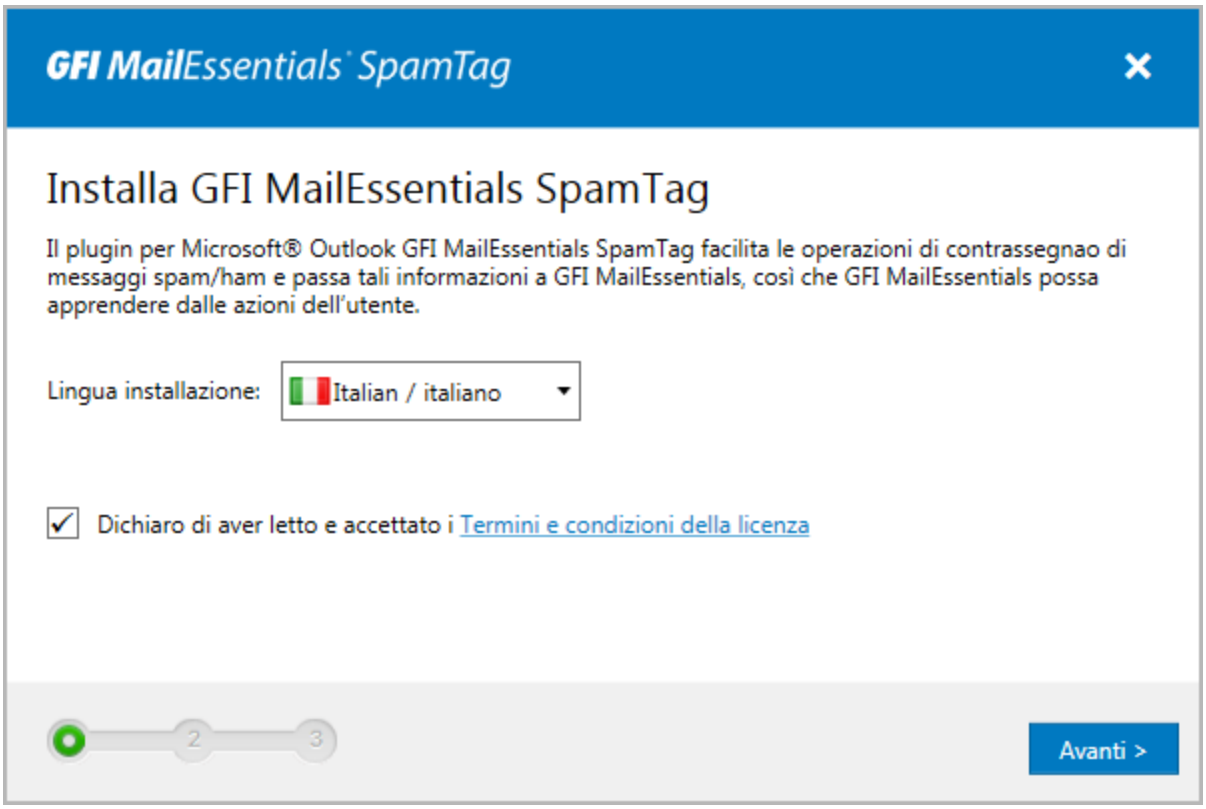
1. Ottenere il programma di installazione di **<cartella di installazione di GFI MailEssentials>/Outlook**.

2. Copiare **GFIMailEssentialsSpamTag.exe** nel computer in cui installare SpamTag.

3. Chiudere Microsoft Outlook.

4. Fare clic con il pulsante destro del mouse sul programma di installazione e selezionare **Esegui come amministratore**.

5. Nella prima schermata, selezionare la lingua per l'installazione.


GFI MailEssentials SpamTag
Installa GFI MailEssentials SpamTag
Il plugin per Microsoft® Outlook GFI MailEssentials SpamTag facilita le operazioni di contrassegnao di messaggi spam/ham e passa tali informazioni a GFI MailEssentials, così che GFI MailEssentials possa apprendere dalle azioni dell'utente.
Lingua installazione:
Italian / italiano
Dichiaro di aver letto e accettato i Termini e condizioni della licenza
2
3
Avanti >

Schermata 93: lingua di installazione di SpamTag e termini della licenza

6. Leggere i **Termini e condizioni della licenza** e, se si concorda, selezionare **Dichiaro di aver letto e accettato i suddetti Termini e condizioni**. Fare clic su **Avanti**.

7. Immettere l'URL utilizzato per connettersi a GFI MailEssentials. Ad esempio: `http://192.168.1.2/MailEssentials` o `http://mygfiserver.mydomin.com/MailEssentials`. Attendere che il programma di installazione verifichi la connessione con GFI MailEssentials tramite l'URL specificato e fare clic su **Avanti**.

8. Specificare il percorso in cui installare SpamTag e fare clic su **Installa**.

9. Al termine, fare clic su **Fine**.

10. Avviare Microsoft Outlook e immettere le credenziali dell'utente.

SpamTag adesso è disponibile nella barra multifunzione di Microsoft Outlook Home (dalla versione 2007 in poi) o nella barra degli strumenti (versione 2003).

Per ulteriori informazioni, selezionare la **Guida** di SpamTag.

6.7.4 Installazione di SpamTag tramite Oggetto Criteri di gruppo

Questa sezione aiuterà a installare in automatico GFI MailEssentials SpamTag su più computer tramite Oggetto Criteri di gruppo. Selezionare l'ambiente del controller di dominio:

» Windows Server 2008 e 2012

» Windows Server 2003

Installazione di SpamTag tramite Oggetto Criteri di gruppo su Windows Server 2008 e 2012

Passaggio 1: Preparazione file MSI e ADM

1. Dal server di GFI MailEssentials accedere alla cartella di installazione di GFI MailEssentialse aprire la sottocartella **Outlook**.

2. Copiare i file MSI e ADM in una cartella condivisa accessibile da tutti gli utenti che hanno installato SpamTag. Accertarsi che gli utenti dispongano almeno di autorizzazioni di lettura alla cartella.

Passaggio 2: Distribuzione di SpamTag

1. Nel controller di dominio, aprire **Server Manager**.

2. Espandere **Server Manager > Caratteristiche > Gestione Criteri di gruppo > Foresta > Domini *nome dominio***. Fare clic con il pulsante destro del mouse sul nome del dominio o su un nome organizzativo e selezionare **Crea un oggetto Criteri di gruppo in questo dominio e crea qui un collegamento...**

3. Immettere un nome per il nuovo oggetto Criteri di gruppo (GPO). Ad esempio: `GFI MailEssentials SpamTag`. Fare clic su **OK**.

4. Fare clic con il pulsante destro del mouse sull'Oggetto Criteri di gruppo, quindi selezionare **Modifica**.

5. Nella finestra **Editor Gestione Criteri di gruppo**, espandere **Configurazione computer > Criteri > Impostazioni software > Installazione software**. Per configurare l'Oggetto criteri di gruppo da installare all'accesso, fare clic con il pulsante destro del mouse su **Installazione software > Nuovo > Pacchetto**.

6. Immettere il percorso di rete della cartella condivisa che contiene il pacchetto MSI SpamTag. Fare clic su **OK**.

> **NOTA**
> Durante la selezione del percorso del file MSI assicurarsi che l'operazione venga effettuata attraverso 'Percorsi di rete', in modo che il nome della condivisione in GFI MailEssentials includa il percorso della condivisione di rete completo piuttosto che il percorso locale.

7. Nel pop-up **Distribuzione del software**, selezionare **Assegnata** e fare clic su **OK**.

8. Il nuovo pacchetto è stato aggiunto in **Installazione software**.

9. Fare clic con il pulsante destro del mouse su **Configurazione computer > Criteri > Modelli amministrativi** e selezionare **Tutte le attività > Aggiunta/Rimozione modelli**.

10. Fare clic su **Aggiungi** e navigare fino alla cartella condivisa contenente **spamtag.adm**.

11. Fare clic su **Chiudi**.

12. Selezionare **Configurazione computer > Criteri > Modelli amministrativi > Modelli amministrativi classici (ADM) > GFI MailEssentials SpamTag**.

13. Dal riquadro a destra, fare doppio clic su **DefaultWebServiceUrl** e selezionare **Attivato**. Digitare l'URL pubblico di GFI MailEssentials in **Indirizzo sito web portale di GFI MailEssentials**. I computer

dove è stato distribuito SpamTag devono essere in grado di connettersi a questo URL tramite il browser web, altrimenti SpamTag non potrà connettersi a GFI MailEssentials.

14. In alternativa, fare clic su **Impostazione precedente** per modificare la lingua predefinita di SpamTag. Fare clic su **Attivato** e modificare il valore **Lingua predefinita**.

15. Fare clic su **OK**.

Passaggio 3: Verifica installazione

Adesso la configurazione dovrebbe essere completa. SpamTag verrà installato al prossimo avvio di ciascun computer client.

Per controllare l'installazione, verificare che la barra degli strumenti di SpamTag sia visibile in Microsoft Outlook® e che si connetta a GFI MailEssentials.

Installazione di SpamTag tramite Windows Server 2003

Passaggio 1: Preparazione file MSI e ADM

1. Dal server di GFI MailEssentials accedere alla cartella di installazione di GFI MailEssentialse aprire la sottocartella **Outlook**.

2. Copiare i file MSI e ADM in una cartella condivisa accessibile da tutti gli utenti che hanno installato SpamTag. Accertarsi che gli utenti dispongano almeno di autorizzazioni di lettura alla cartella.

Passaggio 2: Distribuzione di SpamTag

1. Dal prompt dei comandi, caricare `mmc.exe` per avviare Microsoft Management Console.

2. Selezionare **File > Aggiungi/Rimuovi snap-in…** e fare clic su **Aggiungi...**

3. Selezionare lo snap-in **Editor oggetti Criteri di gruppo** e fare clic su **Aggiungi**.

4. Fare clic su **Sfoglia…** e scegliere i criteri di dominio da modificare.

5. Selezionare i criteri di dominio e scegliere **OK**.

6. Fare clic su **Fine** per chiudere la finestra di dialogo 'Selezione oggetto Criteri di gruppo'. Fare clic su **Chiudi** per chiudere la finestra di dialogo 'Aggiungi snap-in in autonomo', quindi su **OK** per chiudere la finestra di dialogo 'Aggiungi/Rimuovi snap-in' e tornare a Microsoft Management Console.

7. Selezionare **Directory principale console > <criterio dominio> > Configurazione utente**, fare clic con il pulsante destro del mouse su **Modelli amministrativi**, quindi selezionare **Aggiunta/Rimozione modelli…**.

8. Fare clic su **Aggiungi…** e cercare il file ADM presente nella cartella condivisa nel passaggio 1. Fare clic su **Apri**.

9. Per tornare a Microsoft Management Console, fare clic su **Chiudi**.

10. Espandere **Directory principale console > <criterio dominio> > Configurazione utente > Modelli amministrativi > GFI Applications**.

11. Dal riquadro a destra, fare doppio clic su **DefaultWebServiceUrl** e selezionare **Attivato**. Digitare l'URL pubblico di GFI MailEssentials. I computer dove è stato distribuito SpamTag devono essere in grado di connettersi a questo URL tramite il browser web, altrimenti SpamTag non potrà connettersi a GFI MailEssentials.

12. In alternativa, fare clic su **Impostazione precedente** per modificare la lingua predefinita di SpamTag. Fare clic su **Attivato** e modificare il valore **Lingua predefinita**.

13. Fare clic su **OK**.

14. Selezionare **Directory principale console** > **<*criterio dominio*>** > **Configurazione computer** > **Impostazioni del software**.

15. Fare clic con il pulsante destro del mouse su **Installazione software** e selezionare **Nuovo** > **pacchetto…**

16. Nella finestra di dialogo **Apri**, individuare la condivisione dove è stato salvato il file MSI nel passaggio 1.

> **NOTA**
> Durante la selezione del percorso del file MSI assicurarsi che l'operazione venga effettuata attraverso 'Percorsi di rete', in modo che il nome della condivisione in GFI MailEssentials includa il percorso della condivisione di rete completo piuttosto che il percorso locale.

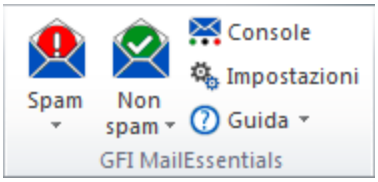
17. Scegliere l'opzione di distribuzione, selezionare **Assegnata** e fare clic su **OK**.

Passaggio 3: Verifica installazione

Adesso la configurazione dovrebbe essere completa. SpamTag verrà installato al prossimo avvio di ciascun computer client.

Per controllare l'installazione, verificare che la barra degli strumenti di SpamTag sia visibile in Microsoft Outlook® e che si connetta a GFI MailEssentials.

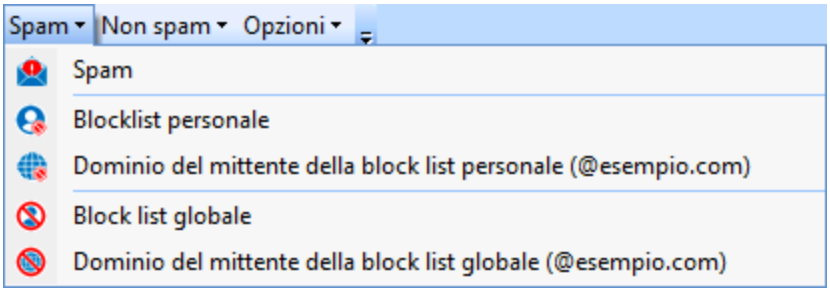
6.7.5 Utilizzo di SpamTag



Schermata 94: SpamTag in Microsoft Outlook 2010

Per informazioni sull'uso di SpamTag, fare riferimento alla guida integrata, facendo clic su **Guida** all'interno di SpamTag.

La guida mostra in automatico le informazioni relative alle funzioni abilitate dall'amministratore nella pagina di impostazioni di SpamTag.



Schermata 95: SpamTag in Microsoft Outlook 2003

6.8 Scansione cartella pubblica

Le tecnologie di spam sono in continua evoluzione e, di conseguenza, si possono riscontrare istanze dove lo spam riesce comunque a superare i filtri antispam, raggiungendo la posta in arrivo del destinatario. Attraverso la scansione cartella pubblica, gli utenti possono classificare manualmente la posta come spam e insegnare a GFI MailEssentials le strutture dello spam, così da classificare la posta simile come tale. I messaggi possono anche essere aggiunti alla whitelist.

IMPORTANTE
Quando il client di rete utilizza Microsoft Outlook come client di posta elettronica, è fortemente consigliato utilizzare GFI MailEssentials SpamTag al posto della scansione cartella pubblica. Per ulteriori informazioni, fare riferimento a SpamTag per Microsoft Outlook (pagina 162).

Funzionamento:

1. Quando viene identificato un messaggio classificato erroneamente (falso positivo o falso negativo), gli utenti lo trascinano nella cartella pubblica appropriata di GFI AntiSpam. Per ulteriori informazioni, fare riferimento a Utilizzo della scansione cartella pubblica (pagina 174).

2. La scansione cartella pubblica recupera i messaggi dalle cartelle pubbliche di GFI AntiSpam e li aggiunge ai database HAM/SPAM.

Le cartelle pubbliche di GFI Antispam devono essere create e configurate sul server di posta. Per ulteriori informazioni, fare riferimento a Abilitazione scansione cartella pubblica (pagina 170)..

6.8.1 Abilitazione scansione cartella pubblica

Per abilitare la scansione cartella pubblica, seguire le istruzioni elencate nelle sezioni seguenti:

- Configurazione della scansione cartella pubblica per Microsoft ® Exchange Server
- Configurazione di un account utente dedicato per Microsoft ® Exchange Server 2003
- Configurazione di un account utente dedicato per Microsoft ® Exchange Server 2007/2010
- Nascondere i post degli utenti nelle cartelle anti-spam GFI

NOTA
È anche possibile utilizzare GFI MailEssentials con Lotus Domino. Per ulteriori informazioni, fare riferimento a Lotus Domino (pagina 32).

Configurazione della scansione cartella pubblica per Microsoft® Exchange Server

1. Dalla console di configurazione di GFI MailEssentials, fare clic su **Antispam > Impostazioni antispam**. Selezionare la scheda **Scansione cartella pubblica**.

2. Fare clic su **Abilita scansione cartella pubblica** e dall'elenco **Eseguire il polling delle cartelle pubbliche tramite** selezionare:

- **Exchange Server 2003**: selezionare MAPI, IMAP o WebDAV.
- **Exchange Server 2007**: selezionare WebDAV o Servizi Web.
- **Exchange Server 2010**: selezionare WebDAV o Servizi Web.

Le opzioni sono descritte nella sottostante tabella.

Opzione	Descrizione
MAPI	Per utilizzare MAPI, GFI MailEssentials deve essere installato in un computer dove è presente Microsoft® Exchange Server. Non è necessario effettuare altre impostazioni.
IMAP	È necessario il servizio IMAP di Microsoft® Exchange. IMAP consente la scansione remota delle cartelle pubbliche e si integra bene negli ambienti che eseguono firewall. Inoltre, IMAP può essere utilizzato con altri server di posta che supportano IMAP. I parametri richiesti sono: » Nome server di posta » Numero di porta (la porta IMAP predefinita è 143) » Nome utente/password » Selezionare l'opzione **Utilizza SSL** per usare una connessione sicura
WebDAV	Indicare il nome del server della posta, la porta (la porta WebDAV predefinita è 80), il nome utente/password e il dominio. Per utilizzare una connessione sicura, selezionare la casella di controllo **Utilizza SSL**. Per impostazione predefinita, le cartelle pubbliche sono accessibili dalla directory virtuale 'public'. Se questa è stata modificata, per specificare il nome directory virtuale corretto per l'accesso alle cartelle pubbliche è necessario modificare il testo nella casella **URL**.
Servizi Web	Specificare i seguenti dettagli: » **Server**: nome server di posta. » **Dominio**: utilizzare il dominio locale. **NOTA:** Se esiste sia un dominio locale che uno pubblico, utilizzare sempre il dominio locale. » **Porta**: la porta predefinita dei servizi Web (80, o 443 se si utilizza SSL). » **Nome utente/password**: utilizzare le credenziali con privilegi amministrativi o creare un utente dedicato da Microsoft® Exchange® Management Shell, a questo scopo immettere il comando seguente per aggiungere le autorizzazioni appropriate: `Add-ADPermission -identity "Archivio cassetta postale" -User NewUser -AccessRights GenericALL` Sostituire `Archivio cassetta postale` con il nome dell'archivio cassetta postale che contiene le cassette postali degli utenti e `NuovoUtente` con il nome utente dell'utente creato. » **Utilizza SSL**: selezionare questa opzione se Servizi Web di Exchange richiede una connessione sicura. Per impostazione predefinita, i servizi Web richiedono SSL. » **URL**: per impostazione predefinita, le cartelle pubbliche sono accessibili dalla directory virtuale 'EWS/exchange.asmx'. Se questa è stata modificata, per specificare il nome directory virtuale corretto per l'accesso alle cartelle pubbliche è necessario modificare il testo nella casella URL. **NOTA:** Si consiglia di verificare le impostazioni manualmente tramite il caricamento dell'URL in un browser Web. Questo dovrebbe caricare un file formattato XML, denominato **services.wsdl**.

3. Per creare automaticamente le cartelle pubbliche, fare clic su **Scansiona adesso**.

4. Se si sta configurando IMAP, WebDAV o Servizi Web, fare clic su **Test**. La notifica sullo schermo confermerà se l'operazione è andata a buon fine. Se la prova ha esito negativo, verificare/aggiornare le credenziali e rieseguire la prova.

5. Fare clic su **Applica**.

Configurazione di un account utente dedicato per Microsoft ® Exchange Server 2003

Per motivi di sicurezza, quando GFI MailEssentials è installato in una DMZ, è consigliabile creare un account utente dedicato per il recupero/scansione dei messaggi dalle cartelle pubbliche.

1. Creare un nuovo utente di Active Directory (AD).

2. Da Gestore di sistema di Microsoft® Exchange, espandere **Cartelle > nodo Cartelle pubbliche**.

3. Fare clic con il pulsante destro del mouse su **Cartelle anti-spam GFI** e selezionare **Proprietà**.

4. Selezionare la scheda **Autorizzazioni** e fare clic su **Autorizzazioni client**.

5. Fare clic su **Aggiungi…**, selezionare il nuovo utente e quindi **OK**.

6. Selezionare il nuovo utente dall'elenco di autorizzazioni client e, sulla base dell'elenco fornito, impostare il ruolo su **Proprietario**. Assicurarsi di aver selezionato tutte le caselle di controllo e che i pulsanti opzione siano impostati su **Tutto**.

7. Fare clic su **OK** per completare la configurazione.

8. Da Gestore di sistema di Microsoft® Exchange, fare clic con il pulsante destro del mouse su **Cartelle anti-spam GFI** e selezionare **Tutte le attività > Propaga impostazioni**.

> **NOTA**
> In Microsoft® Exchange Server 2003 SP2, fare clic con il pulsante destro del mouse su **Cartelle anti-spam GFI** e selezionare l'opzione **Tutte le attività > Gestione impostazioni**.

9. Selezionare **Diritti cartella o Modifica autorizzazioni client** e fare clic su **OK** o **Avanti**.

10. Specificare le credenziali del nuovo account utente avanzato creato nel passaggio 1 e verificare la configurazione per assicurare la correttezza delle autorizzazioni.

Configurazione di un account utente dedicato per Microsoft ® Exchange Server 2007/2010

Durante la configurazione di un account utente dedicato per il recupero dei messaggi dalle cartelle pubbliche antispam di GFI, l'utente dovrà disporre di diritti di accesso da 'proprietario' su tali cartelle.

1. Creare un nuovo utente (avanzato) di Active Directory (AD).

2. Accedere a Microsoft ® Exchange Server utilizzando privilegi amministrativi.

3. Aprire **Microsoft® Exchange Management Shell** ed eseguire il seguente comando:

```
Get-PublicFolder -Identity "\Cartelle anti-spam GFI" -Recurse |
ForEach-Object {Add-PublicFolderClientPermission -Identity $_.Identity
-User "NOMEUTENTE" -AccessRights owner -Server "NOMESERVER"}
```

Cambiare `NOMEUTENTE` e `NOMESERVER` con i dati pertinenti dell'utente Active Directory in questione. Esempio:

```
Get-PublicFolder -Identity "\Cartelle anti-spam GFI" -Recurse |
ForEach-Object {Add-PublicFolderClientPermission -Identity $_.Identity
-User "mesuser" -AccessRights owner -Server "exch07"}
```

Nascondere i post degli utenti nelle cartelle anti-spam GFI

Per motivi di privacy e sicurezza, è consigliabile nascondere i post degli utenti effettuati nelle cartelle anti-spam GFI. In questo modo, gli utenti potranno solo pubblicare nelle cartelle senza poter visualizzare i post esistenti, nemmeno quelli che hanno eseguito personalmente. Per configurare i privilegi degli utenti e nascondere i post agli utenti non autorizzati:

Microsoft ® Exchange 2003

1. Da Gestore di sistema di Microsoft® Exchange, espandere **Cartelle > nodo Cartelle pubbliche**.

2. Fare clic con il pulsante destro del mouse su **Cartelle anti-spam GFI** e selezionare **Proprietà**.

3. Selezionare la scheda **Autorizzazioni** e fare clic su **Autorizzazioni client**.

4. Fare clic su **Aggiungi**… e selezionare l'utente/gruppo da cui nascondere i post, quindi fare clic su **OK**.

5. Selezionare l'utente/gruppo configurato in precedenza dall'elenco di autorizzazioni client e impostarne il ruolo su **Collaboratore**.

6. Assicurarsi che sia selezionato solo **Creazione elementi** e che i pulsanti opzione siano impostati su **Nessuno**.

7. Fare clic su **OK** per completare la configurazione.

8. Da Gestore di sistema di Microsoft® Exchange, fare clic con il pulsante destro del mouse su **Cartelle anti-spam GFI** e selezionare **Tutte le attività > Propaga impostazioni**.

9. Selezionare la casella di controllo **Diritti cartella** e fare clic su **OK**.

Microsoft® Exchange 2007

1. In **Microsoft® Exchange Management Shell**, digitare il seguente comando:

```
ReplaceUserPermissionOnPFRecursive.ps1 -Server "server" -
TopPublicFolder "\'Cartelle anti-spam GFI'" -User "Default" -
Permissions Contributor
```

Sostituire "`server`" con il nome completo del computer.

2. Quando richiesto, digitare `y` per confermare le autorizzazioni per ogni cartella.

Questo comando imposterà le autorizzazioni predefinite per le cartelle pubbliche di GFI MailEssentials per il collaboratore: gli utenti potranno spostare le e-mail in Cartelle pubbliche ma non potranno visualizzare né modificare le voci. Per impostazione predefinita, gli amministratori sono i proprietari delle cartelle pubbliche e ne possono visualizzare o modificare le voci. Per ulteriori informazioni sulle autorizzazioni per le cartelle pubbliche, fare riferimento a:

http://go.gfi.com/?pageid=ME_PFPermissionsExch2007

Microsoft® Exchange 2010

1. In Microsoft ® Exchange Management Shell, modificare la cartella con quella di script di Microsoft® Exchange, presente nella cartella di installazione di Microsoft® Exchange. Se Microsoft® Exchange è installato nel percorso predefinito, la cartella script si troverà qui:

```
C:\Program Files\Microsoft\Exchange Server\V14\Scripts\
```

2. Digitare il comando seguente:

```
ReplaceUserPermissionOnPFRecursive.ps1 -Server "server" -
TopPublicFolder "\Cartelle anti-spam GFI" -User "Default" -Permissions
Contributor
```

Sostituire "`server`" con il nome completo del computer.

Questo comando imposterà le autorizzazioni predefinite per le cartelle pubbliche di GFI MailEssentials per il collaboratore: gli utenti potranno spostare le e-mail in Cartelle pubbliche ma non potranno visualizzare né modificare le voci. Per impostazione predefinita, gli amministratori sono i proprietari delle cartelle pubbliche e ne possono visualizzare o modificare le voci. Per ulteriori informazioni sulle autorizzazioni per le cartelle pubbliche, fare riferimento a:

http://go.gfi.com/?pageid=ME_PFPermissionsExch2010

6.8.2 Utilizzo della scansione cartella pubblica

Verifica messaggi spam

1. Quando i messaggi spam vengono recapitati nella cassetta postale dell'utente (nella cartella Posta in arrivo, Posta indesiderata o in una cartella personalizzata), indicare agli utenti singoli di posta elettronica di effettuare un controllo periodico dei messaggi spam.

2. Possono esserci dei casi in cui i messaggi attendibili vengono erroneamente identificati come spam (falsi positivi). Per ulteriori informazioni, fare riferimento a Gestione posta attendibile (pagina 174).

3. Possono esserci anche dei casi dove i messaggi spam non vengono rilevati (falsi negativi). Per ulteriori informazioni, fare riferimento a Gestione dello spam (pagina 175).

Gestione posta attendibile

Come per ogni soluzione antispam, GFI MailEssentials potrebbe richiedere tempo prima di ottenere le condizioni di filtraggio antispam ottimali. Se non sono state ancora raggiunte, possono verificarsi dei casi in cui la posta attendibile viene identificata come spam.

In questi casi, gli utenti devono aggiungere nelle cartelle **Aggiungi alla whitelist** e **Messaggio attendibile** i messaggi erroneamente identificati come spam, così da insegnare a GFI MailEssentials che il messaggio in questione non è spam.

> **NOTE**
> 1. In Microsoft® Outlook, l'operazione di trascinamento sposta la posta nella cartella selezionata. Per conservare una copia del messaggio, tenere premuto il tasto CTRL per copiare il messaggio anziché spostarlo.
> 2. In questo manuale sono incluse informazioni dettagliate su come creare le cartelle anti-spam GFI. Per ulteriori informazioni, fare riferimento a Abilitazione scansione cartella pubblica (pagina 170)..

Aggiunta di mittenti alla whitelist

1. Nell'elenco cartelle pubbliche del client di posta (ad esempio, Microsoft® Outlook), individuare la cartella pubblica **Cartelle anti-spam GFI > Aggiungi alla whitelist**.

2. Trascinare i messaggi o le newsletter nella cartella pubblica **Aggiungi alla whitelist**.

Aggiunta di elenchi di discussione alla whitelist

I messaggi inviati agli elenchi di discussione devono avere l'indirizzo e-mail dell'elenco di discussione come destinatario del messaggio. Per ricevere i messaggi di posta da elenchi di discussione specifici, l'indirizzo e-mail dell'elenco deve essere inserito nella whitelist.

1. Utilizzando il client di posta elettronica, (esempio, Microsoft® Outlook), individuare la cartella pubblica **Cartelle anti-spam GFI > Elenco discussione scelto**.

2. Trascinare gli elenchi discussione nella cartella pubblica **Elenco discussione scelto**.

Utilizzo dei messaggi spam per istruire il filtro bayesiano

1. Nelle cartelle pubbliche del client di posta (ad esempio, Microsoft® Outlook), individuare la cartella

pubblica **Cartelle anti-spam GFI > Messaggio attendibile**.

2. Trascinare i messaggi di posta nella carella **Messaggio attendibile**.

Gestione dello spam

Anche se GFI MailEssentials inizia l'identificazione di messaggi spam come standard, possono esserci dei casi in cui lo spam arriva nelle cassette postali degli utenti senza essere rilevato. Normalmente, questo potrebbe essere dovuto alle impostazioni di configurazione che non sono state ancora eseguite o a nuovi tipi di spam a cui GFI MailEssentials non si è ancora adattato. In entrambi i casi, queste situazioni vengono risolte quando GFI MailEssentials viene configurato per l'acquisizione di questo tipo di spam.

In questi casi, gli utenti devono aggiungere tali messaggi alle cartelle **Aggiungi a block list** e **Messaggio spam**, così da insegnare a GFI MailEssentials che il messaggio in questione è spam.

> **NOTE**
> 1. In Microsoft® Outlook, l'operazione di trascinamento sposta la posta nella cartella selezionata. Per conservare una copia del messaggio, tenere premuto il tasto CTRL per copiare il messaggio anziché spostarlo.
> 2. In questo manuale sono incluse informazioni dettagliate su come creare le cartelle anti-spam GFI. Per ulteriori informazioni, fare riferimento a Abilitazione scansione cartella pubblica (pagina 170)..

Aggiunta di mittenti alla block list e-mail

1. Nell'elenco cartelle pubbliche del client di posta (ad esempio, Microsoft® Outlook), individuare la cartella pubblica **Cartelle anti-spam GFI > Aggiungi a block list**.

2. Trascinare i messaggi di posta nella cartella **Aggiungi a block list**.

Utilizzo dei messaggi spam per istruire il filtro bayesiano

1. Nelle cartelle pubbliche del client di posta (ad esempio, Microsoft® Outlook), individuare la cartella pubblica **Cartelle anti-spam GFI > Messaggio spam**.

2. Trascinare il messaggio spam nella cartella **Messaggio spam**.

7 Filtro contenuti

I motori di Filtro contenuti consentono agli amministratori di controllare il contenuto dei messaggi. Questi motori scansionano il contenuto di messaggi e allegati e bloccano i messaggi il cui contenuto corrisponde alle regole di filtro contenuti.

Argomenti del presente capitolo:

7.1 Filtro parola chiave **176**

7.2 Filtro allegati **183**

7.3 Filtro avanzato contenuto **190**

7.4 Motore di decompressione **196**

7.1 Filtro parola chiave

Filtro parole chiave consente di impostare regole che filtrano i messaggi contenenti parole chiave specifiche o una combinazione di parole chiave nel corpo o nell'oggetto del messaggio. Una regola è composta da:

- Parole chiave da bloccare nel corpo, oggetto o allegato del messaggio.
- Azioni da attuare quando viene individuata una parola chiave.
- Gli utenti a cui viene applicata una regola.

Per configurare le regole del contenuto, selezionare **Filtro contenuti > Filtro parola chiave**. Questa pagina consente all'utente di visualizzare, creare, abilitare, disabilitare o eliminare le regole.

7.1.1 Creazione regola filtro parola chiave

Per creare una regola di Filtro parola chiave, attenersi ai passaggi elencati di seguito:

- Passaggio 1: configurazione delle impostazioni di base della regola
- Passaggio 2: configurazione dei termini da bloccare
- Passaggio 3: configurazione delle azioni da intraprendere sui messaggi rilevati
- Passaggio 4: indicazione degli utenti a cui applicare questa regola

Passaggio 1: configurazione delle impostazioni di base della regola

1. Selezionare **Filtro contenuti > Filtro parola chiave** e fare clic su **Aggiungi regola...**
2. Nella casella di testo **Nome regola** specificare un nome per la regola.
3. Scegliere se scansionare i messaggi in entrata, in uscita e/o interni.

Opzione	Descrizione
Controlla messaggi di posta in arrivo	Selezionare l'opzione per scansionare i messaggi in entrata.

Opzione	Descrizione
Controlla messaggi di posta in uscita	Selezionare l'opzione per scansionare i messaggi in uscita.
Controlla e-mail interne	Selezionare questa opzione per scansionare i messaggi interni. **NOTA** Questa opzione è disponibile solo quando GFI MailEssentials è installato in un computer Microsoft® Exchange Server.

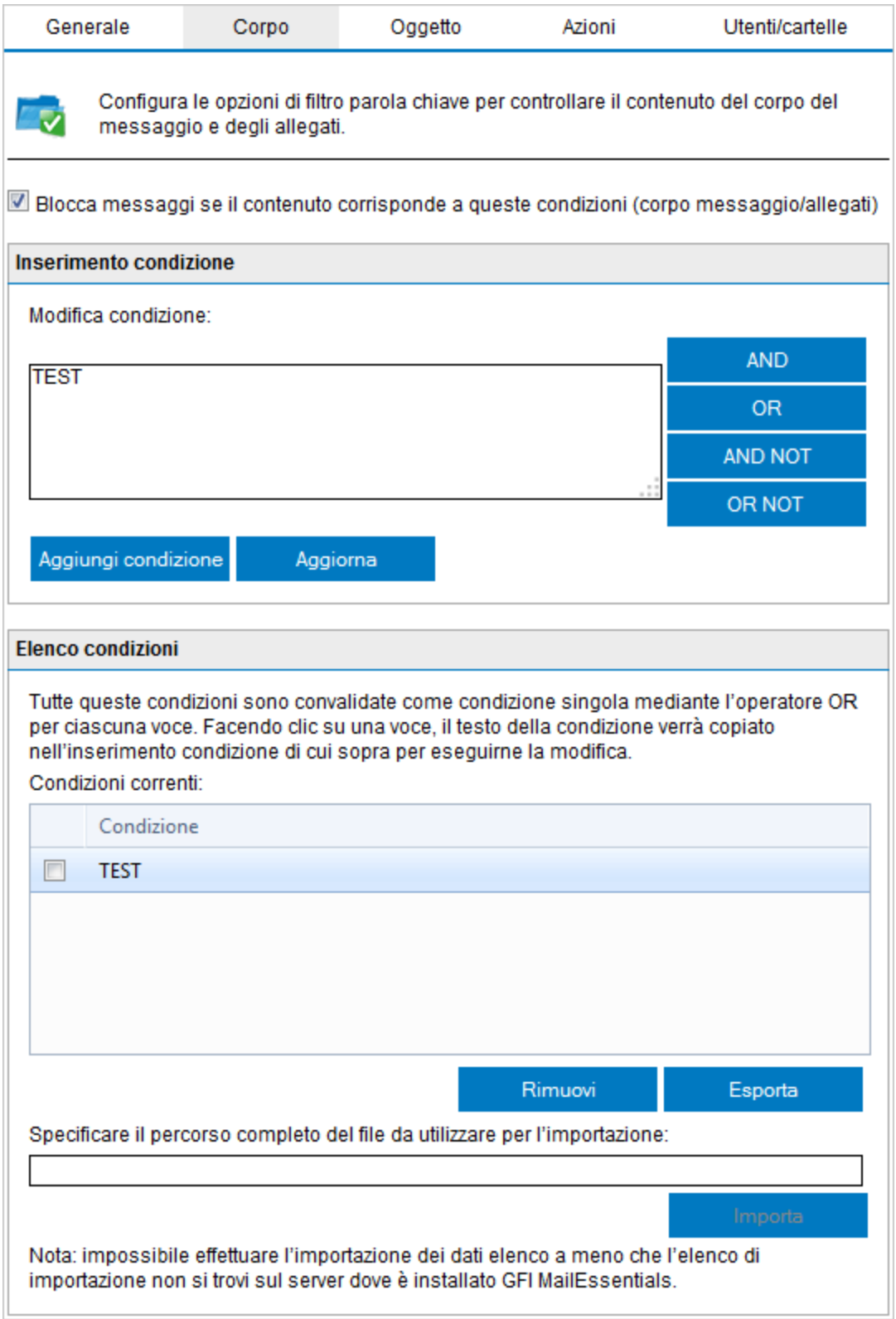
4. Per bloccare i messaggi crittografati con la tecnologia PGP, selezionare **Blocca i messaggi con crittografia PGP**.

> **NOTA**
> La crittografia PGP è un sistema crittografico a chiave pubblica spesso utilizzato per crittografare i messaggi.

Passaggio 2: configurazione dei termini da bloccare

1. Selezionare la scheda **Corpo** per indicare le parole chiave presenti nel corpo del messaggio da bloccare.

2. Selezionare **Blocca messaggi se il contenuto corrisponde a queste condizioni (corpo messaggio/allegati)** per consentire la scansione del corpo alla ricerca di parole chiave.


Generale
Corpo
Oggetto
Azioni
Utenti/cartelle
Configura le opzioni di filtro parola chiave per controllare il contenuto del corpo del messaggio e degli allegati.
Blocca messaggi se il contenuto corrisponde a queste condizioni (corpo messaggio/allegati)
Inserimento condizione
Modifica condizione:
TEST
AND
OR
AND NOT
OR NOT
Aggiungi condizione
Aggiorna
Elenco condizioni
Tutte queste condizioni sono convalidate come condizione singola mediante l'operatore OR per ciascuna voce. Facendo clic su una voce, il testo della condizione verrà copiato nell'inserimento condizione di cui sopra per eseguirne la modifica.
Condizioni correnti:
Condizione
TEST
Rimuovi
Esporta
Specificare il percorso completo del file da utilizzare per l'importazione:
Importa
Nota: impossibile effettuare l'importazione dei dati elenco a meno che l'elenco di importazione non si trovi sul server dove è installato GFI MailEssentials.

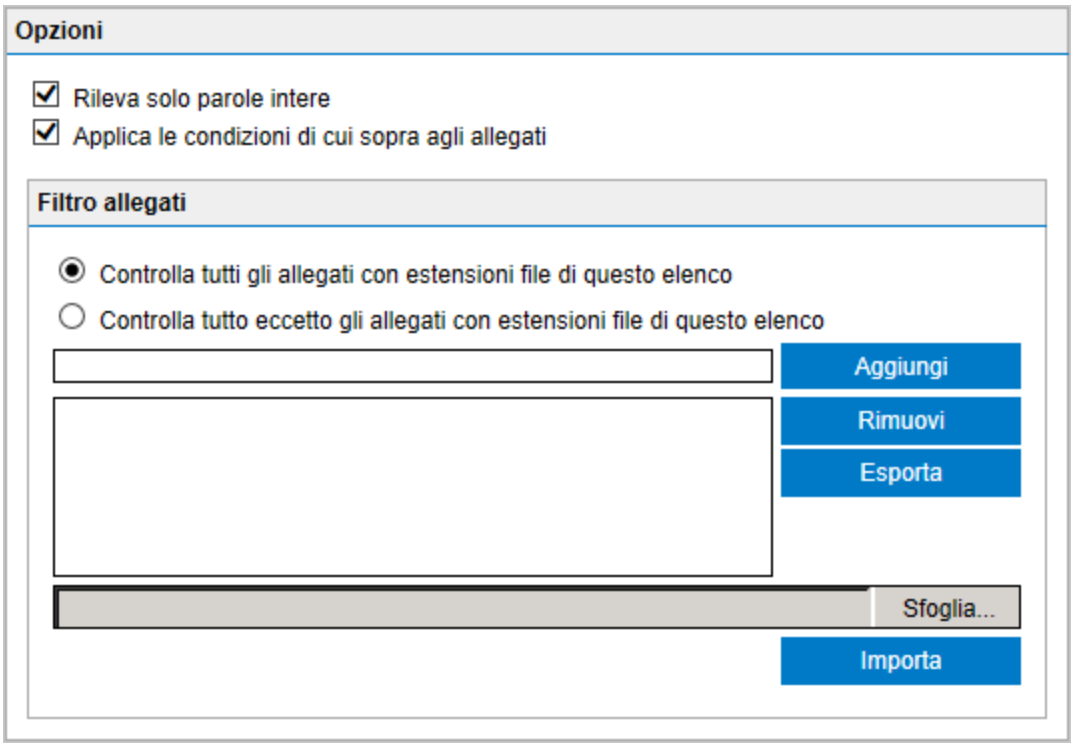
Schermata 96: filtro contenuti: scheda Corpo - configurazione condizioni

3. Nell'area **Inserimento condizione**, digitare le parole chiave da bloccare nella casella **Modifica condizione**. È anche possibile utilizzare le condizioni **AND**, **OR**, **AND NOT** e **OR NOT** per utilizzare una combinazione di parole chiave.

4. Per aggiungere la parola chiave o la combinazione di parole chiave digitate, fare clic su **Aggiungi condizione**.

Per modificare una voce nell'elenco **Condizioni**, selezionarla e apportare le modifiche necessarie nella casella **Inserimento condizione**. Per rimuovere una voce dall'elenco **Condizioni**, selezionarla e fare clic su **Rimuovi**.

Per applicare le modifiche, fare clic su **Aggiorna**.



Schermata 97: filtro contenuti: scheda Corpo - configurazione altre opzioni

5. (Facoltativo) Dall'area **Opzioni**, configurare le seguenti impostazioni:

Opzione	Descrizione
Rileva solo parole intere	Bloccare i messaggi quando le parole chiave specificate corrispondono a parole intere.
Applica le condizioni di cui sopra agli allegati	Selezionare questa opzione per applicare la regola anche al testo negli allegati. Nell'area **Filtro allegati**, indicare l'estensione file degli allegati (ad esempio, `.doc`) da applicare o escludere dalla regola.

6. Selezionare la scheda **Oggetto** per indicare le parole chiave da bloccare nell'oggetto del messaggio.

7. Nell'area **Inserimento condizione**, digitare le parole chiave da bloccare nella casella **Modifica condizione**. È anche possibile utilizzare le condizioni **AND**, **OR**, **AND NOT** e **OR NOT** per utilizzare una combinazione di parole chiave.

8. Per aggiungere la parola chiave o la combinazione di parole chiave digitate, fare clic su **Aggiungi condizione**.

Per modificare una voce nell'elenco **Condizioni**, selezionarla e apportare le modifiche necessarie nella casella **Inserimento condizione**. Per rimuovere una voce dall'elenco **Condizioni**, selezionarla e fare clic su **Rimuovi**.

Per applicare le modifiche, fare clic su **Aggiorna**.

9. Dall'area **Opzioni**, configurare la modalità di associazione delle parole chiave. Selezionare **Rileva solo parole intere** per bloccare i messaggi dove le parole chiave indicate corrispondono a parole

intere nell'oggetto.

Passaggio 3: configurazione delle azioni da intraprendere sui messaggi rilevati

1. Fare clic sulla scheda **Azioni** per configurare l'operazione da effettuare quando si attiva questa regola.

2. Per bloccare un messaggio che rispetta le condizioni della regola, selezionare **Blocca e-mail ed esegui l'azione seguente**, quindi fare clic su una delle seguenti opzioni:

Opzione	Descrizione
E-mail in quarantena	Archivia i messaggi bloccati in Quarantine Store. I messaggi inseriti in quarantena potranno essere successivamente rivisti (per approvazione/eliminazione). Per ulteriori informazioni, fare riferimento a Quarantena (pagina 203).
Elimina e-mail	Elimina i messaggi di posta bloccati.
Sposta nella cartella su disco	Sposta il messaggio in una cartella su disco. Digitare il percorso completo della cartella dove salvare i messaggi bloccati.

IMPORTANTE
Le azioni interessano sempre l'intero messaggio il cui contenuto è bloccato, anche in presenza di altro contenuto (come gli allegati) che non attiva questa regola.

NOTA
Quando GFI MailEssentials viene installato sullo stesso computer di Microsoft® Exchange 2003, GFI MailEssentials potrebbe non riuscire a bloccare i messaggi in uscita ma invece sostituire il contenuto bloccato con un rapporto sulle minacce.

3. Selezionare **Invia una copia disinfettata del messaggio originale ai destinatari** per scegliere se inviare ai destinatari una copia del messaggio bloccato, privo dei contenuti dannosi.

4. GFI MailEssentials può inviare notifiche di posta ogni volta che un messaggio attiva questo filtro. Per abilitare questa funzione, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Notifica amministratore	Notifica l'amministratore quando questo motore blocca un messaggio. Per ulteriori informazioni, fare riferimento a Indirizzo e-mail amministratore (pagina 241).
Notifica utente locale	Notifica il messaggio bloccato ai destinatari locali del messaggio.

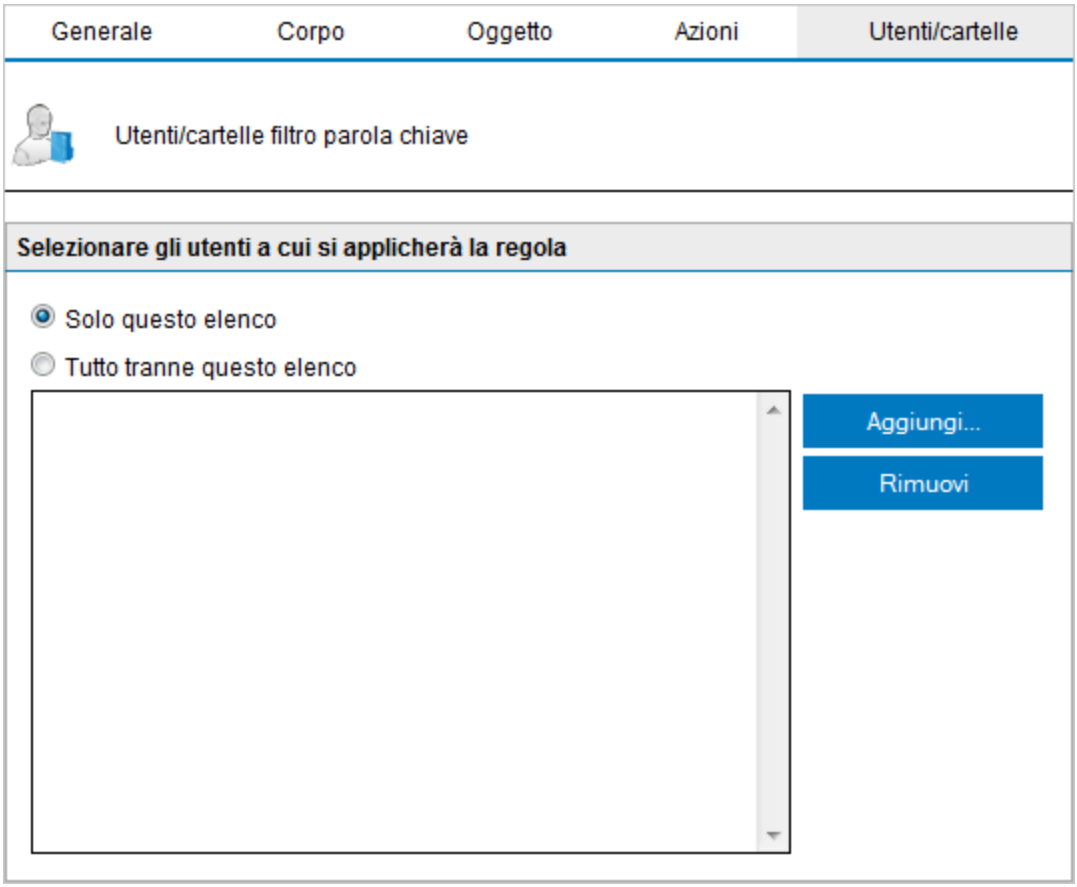
5. Per registrare l'attività di questo motore in un file di registro, selezionare **Registra occorrenze nel seguente file**. Nella casella di testo, indicare il percorso e il nome del file di una posizione personalizzata su disco dove è possibile salvare il file di registro. Per impostazione predefinita, i file di registro vengono archiviati in:

```
<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\EmailSecurity\Logs\<nome motore>.log
```

Passaggio 4: indicazione degli utenti a cui applicare questa regola

1. Per impostazione predefinita, questa regola viene applicata a tutti gli utenti della posta. Tuttavia,

GFI MailEssentials permette di applicare questa regola a un elenco personalizzato di utenti della posta indicati nella scheda Utenti/Cartelle.

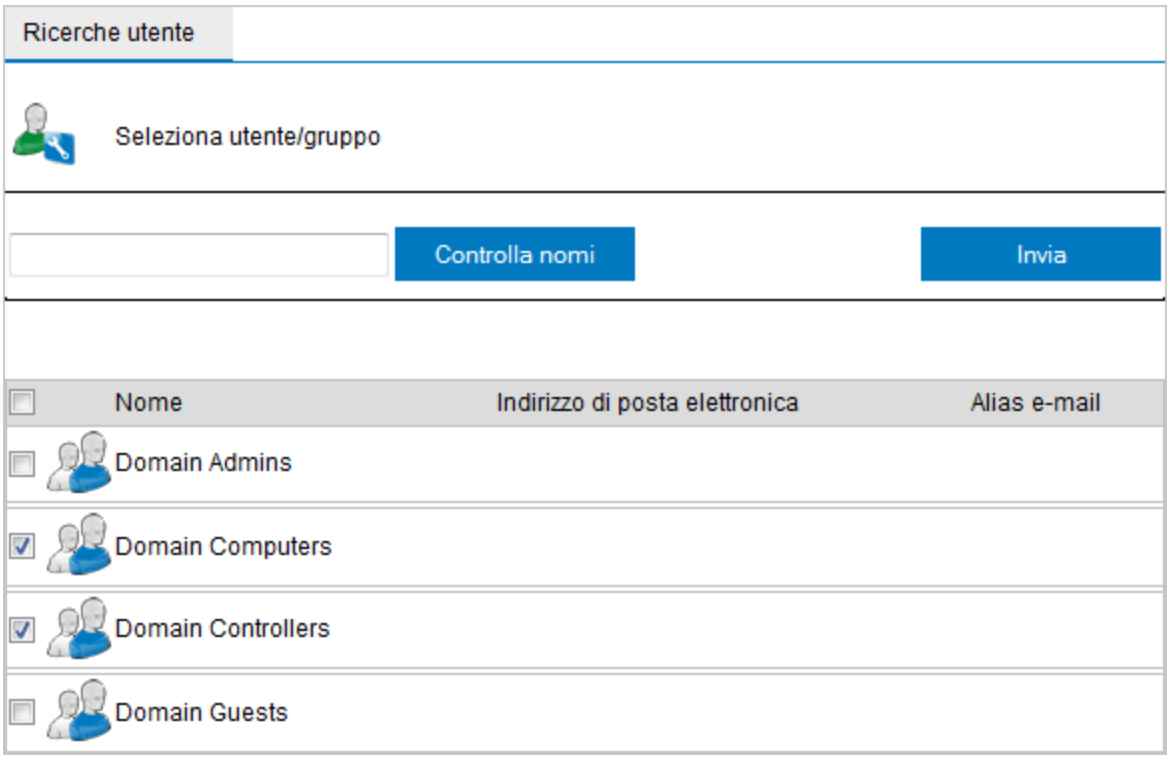


Schermata 98: Filtro contenuti: scheda Utenti/cartelle

2. Indicare gli utenti a cui applicare questa regola.

Opzione	Descrizione
Solo questo elenco	Applicare questa regola a un elenco personalizzato di utenti della posta, gruppi o cartelle pubbliche.
Tutto tranne questo elenco	Applicare questa regola a tutti gli utenti della posta, ad eccezione degli utenti, gruppi o cartelle pubbliche indicati in questo elenco.

3. Per aggiungere utenti della posta, gruppi di utenti e/o cartelle pubbliche all'elenco, fare clic su **Aggiungi**.



Schermata 99: Aggiunta di utenti a una regola di filtro dei contenuti

4. Nella finestra di dialogo **Ricerche utente**, inserire il nome dell'utente/gruppo di utenti di posta o della cartella pubblica da aggiungere, quindi fare clic su **Controlla nomi**. Di seguito verranno elencati i risultati trovati in utenti, gruppi o cartelle pubbliche.

> **NOTA**
> Non è necessario inserire il nome completo di utenti, gruppi o cartella pubblica. È sufficiente inserire una parte del nome. GFI MailEssentials elencherà tutti i nomi contenenti i caratteri specificati. Ad esempio, digitando `sco`, GFI MailEssentials verranno restituiti nomi come `Scott Adams` e `Freeman Prescott`, se disponibili.

5. Selezionare la casella di spunta accanto al nome da aggiungere all'elenco, quindi fare clic su **OK**.

> **NOTA**
> Per rimuovere le voci dall'elenco, selezionare l'utente/gruppo di utenti/cartella pubblica da rimuovere e fare clic su **Rimuovi**.

6. Ripetere i passaggi da 3 a 5 per aggiungere all'elenco tutti gli utenti necessari.

7. Fare clic su **Applica**.

7.1.2 Abilitazione/disabilitazione regole

Per abilitare/disabilitare le regole di filtro dei contenuti:

1. Selezionare **Filtro contenuti > Filtro parola chiave**.

2. Dalla pagina **Filtro contenuti**, selezionare la casella di controllo delle regole da abilitare o

disabilitare.

3. Fare clic su **Abilita selezionati** o **Disabilita selezionati**.

7.1.3 Rimozione regole di filtro dei contenuti

> **AVVISO**
> Le regole eliminate non sono recuperabili. Nel dubbio, si consiglia di disabilitare una regola.

1. Selezionare **Filtro contenuti > Filtro parola chiave**.
2. Dalla pagina Filtro contenuti, selezionare la casella di controllo delle regole da rimuovere.
3. Fare clic su **Rimuovi selezionati**.

7.1.4 Modifica di una regola esistente

1. Selezionare **Filtro contenuti > Filtro parola chiave**.
2. Dalla pagina **Filtro contenuti**, fare clic sul nome della regola da modificare.
3. Eseguire le modifiche richieste nelle proprietà della regola, quindi fare clic su **Applica**.

7.1.5 Modifica priorità regola

Le regole del Filtro contenuti vengono applicate nel medesimo ordine, dall'inizio alla fine nel modo in cui sono elencate nella pagina Filtro contenuti (ovvero, viene controllata per prima una regola con il valore di priorità 1). Per modificare la sequenza/priorità delle regole:

1. Selezionare **Filtro contenuti > Filtro parola chiave**.
2. Dalla pagina **Filtro contenuti**, fare clic sulle frecce ↑ (su) o ↓ (giù) per aumentare o diminuire rispettivamente la priorità della regola.
3. Ripetere il passaggio 2 finché le regole non sono collocate nella sequenza desiderata.

7.2 Filtro allegati

Filtro allegati consente la configurazione di regole per il filtraggio dei tipi di allegati dei messaggi da autorizzare e bloccare sul server di posta. Una regola è composta da:

- Tipi di allegato da bloccare
- Azioni da attuare quando viene individuato un allegato corrispondente
- Gli utenti a cui viene applicata una regola.

Per configurare le regole dell'allegato, selezionare **Filtro contenuti > Filtro allegati**. Questa pagina consente all'utente di visualizzare, creare, abilitare, disabilitare o eliminare le regole.

7.2.1 Creazione di una regola filtro allegati

Per creare una regola di Filtro allegati, attenersi ai passaggi elencati di seguito:

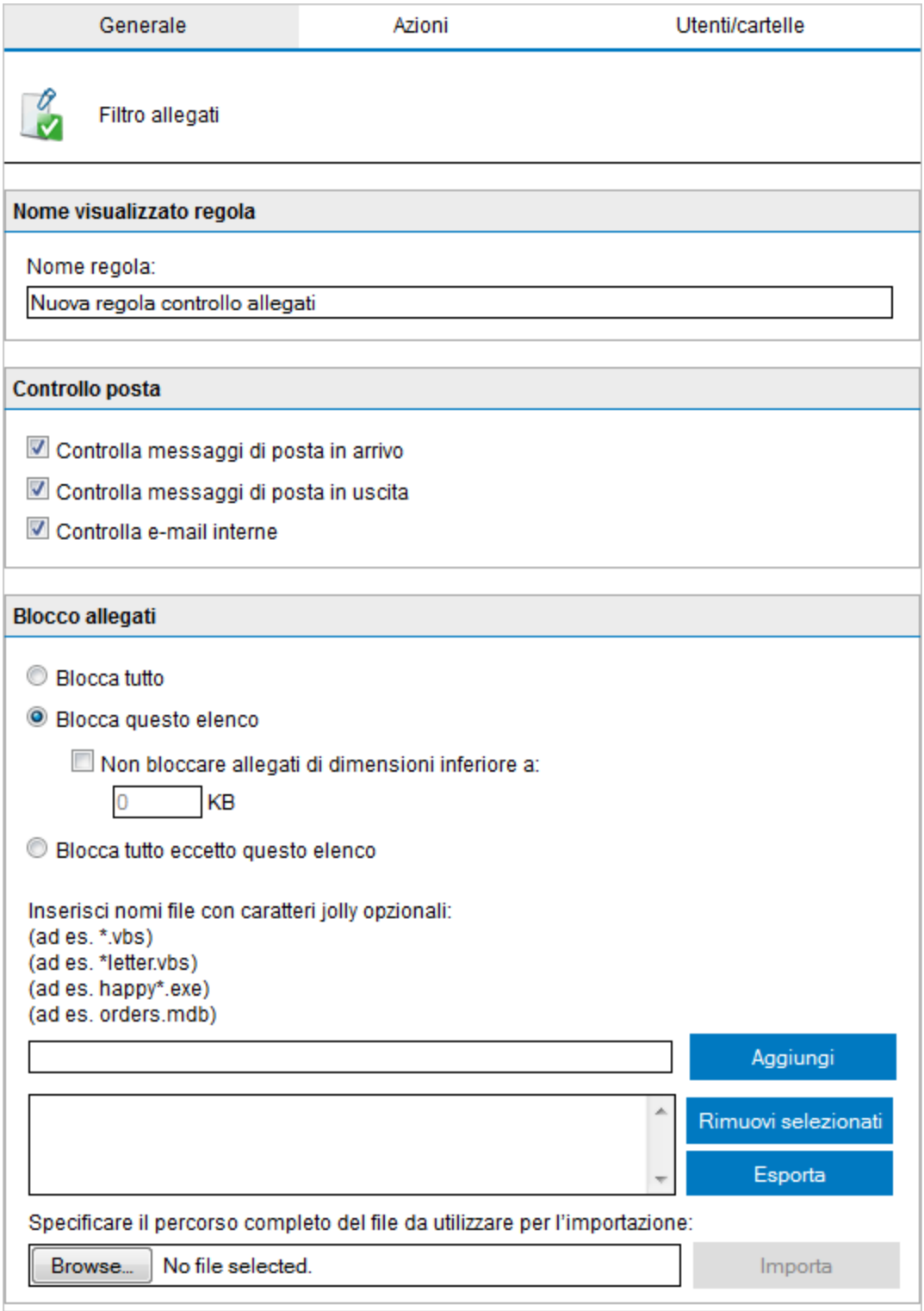
- Passaggio 1: configurazione delle impostazioni di base delle regole e dei termini da bloccare
- Passaggio 2: configurazione delle azioni da intraprendere sui messaggi rilevati

» Passaggio 3: indicazione degli utenti a cui applicare questa regola

Passaggio 1: configurazione delle impostazioni di base delle regole e dei termini da bloccare

1. Selezionare **Filtro contenuti > nodo Filtro allegati.**

2. Fare clic su **Aggiungi regola....**



Schermata 100: filtro allegati: scheda Generale

3. Nella casella di testo **Nome regola** specificare un nome per la regola.

4. Scegliere se scansionare i messaggi in entrata, in uscita e/o interni.

Opzione	Descrizione
Controlla messaggi di posta in arrivo	Selezionare l'opzione per scansionare i messaggi in entrata.
Controlla messaggi di posta in uscita	Selezionare l'opzione per scansionare i messaggi in uscita.
Controlla e-mail interne	Selezionare questa opzione per scansionare i messaggi interni. **NOTA** Questa opzione è disponibile solo quando GFI MailEssentials è installato in un computer Microsoft® Exchange Server.

5. Nell'area **Blocco allegati**, specificare i tipi di allegati da bloccare:

Opzione	Descrizione
Blocca tutto	Blocca tutti gli allegati dei messaggi di qualsiasi tipo.
Blocca questo elenco	Blocca un elenco personalizzato di tipi di allegati. Digitare un nome file e/o un tipo di allegato da bloccare nella casella di testo **Inserisci nomi file con caratteri jolly opzionali**, quindi fare clic su **Aggiungi**. Ripetere la procedura per tutti i nomi file e/o tipi di allegati da bloccare.
Non bloccare allegati di dimensioni inferiore a:	Selezionare questa opzione per consentire i tipi di allegati nell'elenco che sono inferiori a una dimensione specifica. Specificare le dimensioni (in KB) nella casella di testo indicata.
Blocca tutto eccetto questo elenco	Blocca tutti gli allegati ad eccezioni di quelle nell'elenco sottostante. Digitare un nome file e/o un tipo di allegato da consentire nella casella di testo **Inserisci nomi file con caratteri jolly opzionali**, quindi fare clic su **Aggiungi**. Ripetere la procedura per tutti i nomi file e/o tipi di allegati da escludere.

NOTA

Quando si specificano i nomi file e/o i tipi di allegati, è possibile utilizzare i caratteri jolly con l'asterisco (*). Ad esempio, indicando `*ordini*.mdb` ci si riferisce a tutti i file del tipo **mdb** che contengono la stringa `ordini` nel nome del file. Indicando `*.jpg` si bloccheranno tutte le immagini del tipo **jpg**.

NOTA

Per rimuovere una voce dall'elenco, selezionarla e fare clic su **Rimuovi selezionati**.

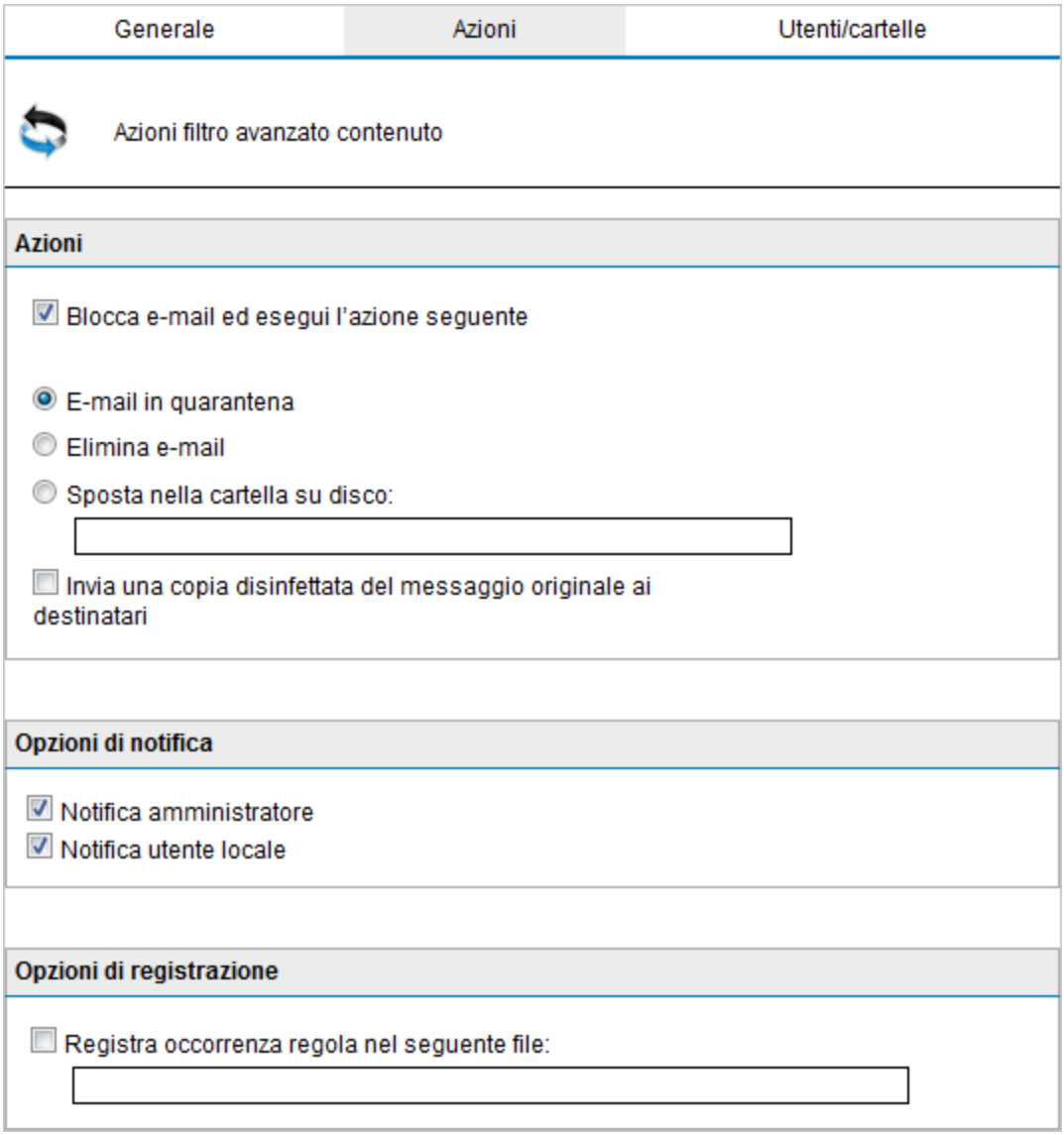
6. È anche possibile bloccare gli allegati di dimensioni maggiori a quelle specificate. Per abilitare questa opzione, dall'area **Opzioni** selezionare **Blocca tutti gli allegati superiori alle seguenti dimensioni in KB** e indicare le dimensioni massime dell'allegato (in KB).

NOTA

Questa funzione blocca tutti gli allegati con dimensioni file superiori a quelle indicate, a prescindere dal fatto che l'allegato corrisponda a una voce dell'elenco **Blocco allegati**.

Passaggio 2: configurazione delle azioni da intraprendere sui messaggi rilevati

1. Fare clic sulla scheda **Azioni** per configurare quello che accade quando si attiva questa regola.



Schermata 101: filtro allegati: scheda Azioni

2. Per bloccare un messaggio che rispetta le condizioni della regola, selezionare **Blocca allegato ed esegui l'azione:**, quindi fare clic su una delle seguenti opzioni:

Opzione	Descrizione
E-mail in quarantena	Archivia i messaggi bloccati in Quarantine Store. I messaggi inseriti in quarantena potranno essere successivamente rivisti (per approvazione/eliminazione). Per ulteriori informazioni, fare riferimento a Quarantena (pagina 203).
Elimina e-mail	Elimina i messaggi di posta bloccati.
Sposta nella cartella su disco	Sposta il messaggio in una cartella su disco. Digitare il percorso completo della cartella dove salvare i messaggi bloccati.

IMPORTANTE

Le azioni interessano sempre l'intero messaggio il cui contenuto è bloccato, anche in presenza di altro contenuto (come gli allegati) che non attiva questa regola.

NOTA

Quando GFI MailEssentials viene installato sullo stesso computer di Microsoft® Exchange 2003, GFI MailEssentials potrebbe non riuscire a bloccare i messaggi in uscita ma invece sostituire il contenuto bloccato con un rapporto sulle minacce.

3. Selezionare **Invia una copia disinfettata del messaggio originale ai destinatari** per scegliere se inviare ai destinatari una copia del messaggio bloccato, privo dei contenuti dannosi.

4. GFI MailEssentials può inviare notifiche di posta ogni volta che un messaggio attiva questo filtro. Per abilitare questa funzione, selezionare una delle seguenti opzioni:

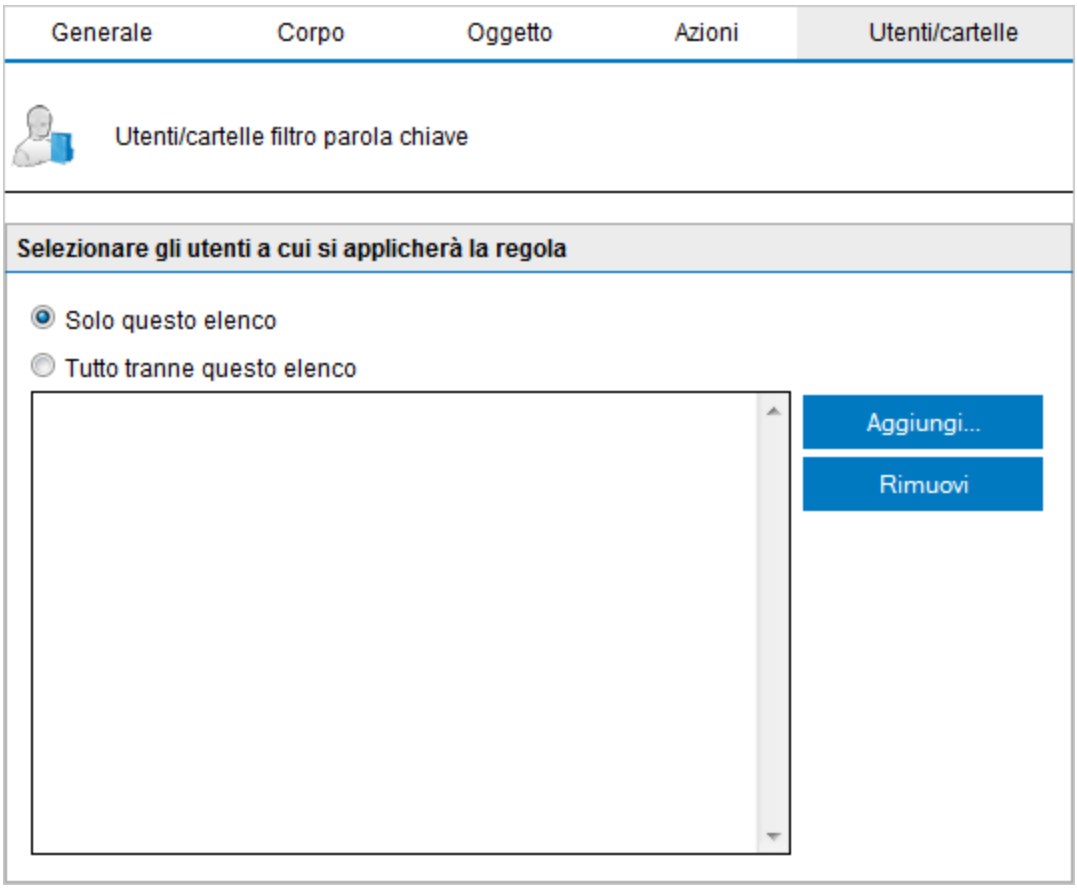
Opzione	Descrizione
Notifica amministratore	Notifica l'amministratore quando questo motore blocca un messaggio. Per ulteriori informazioni, fare riferimento a Indirizzo e-mail amministratore (pagina 241).
Notifica utente locale	Notifica il messaggio bloccato ai destinatari locali del messaggio.

5. Per registrare l'attività di questo motore in un file di registro, selezionare **Registra occorrenze nel seguente file**. Nella casella di testo, indicare il percorso e il nome del file di una posizione personalizzata su disco dove è possibile salvare il file di registro. Per impostazione predefinita, i file di registro vengono archiviati in:

<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\EmailSecurity\Logs\<nome motore>.log

Passaggio 3: indicazione degli utenti a cui applicare questa regola

1. Per impostazione predefinita, questa regola viene applicata a tutti gli utenti della posta. Tuttavia, GFI MailEssentials permette di applicare questa regola a un elenco personalizzato di utenti della posta indicati nella scheda Utenti/Cartelle.

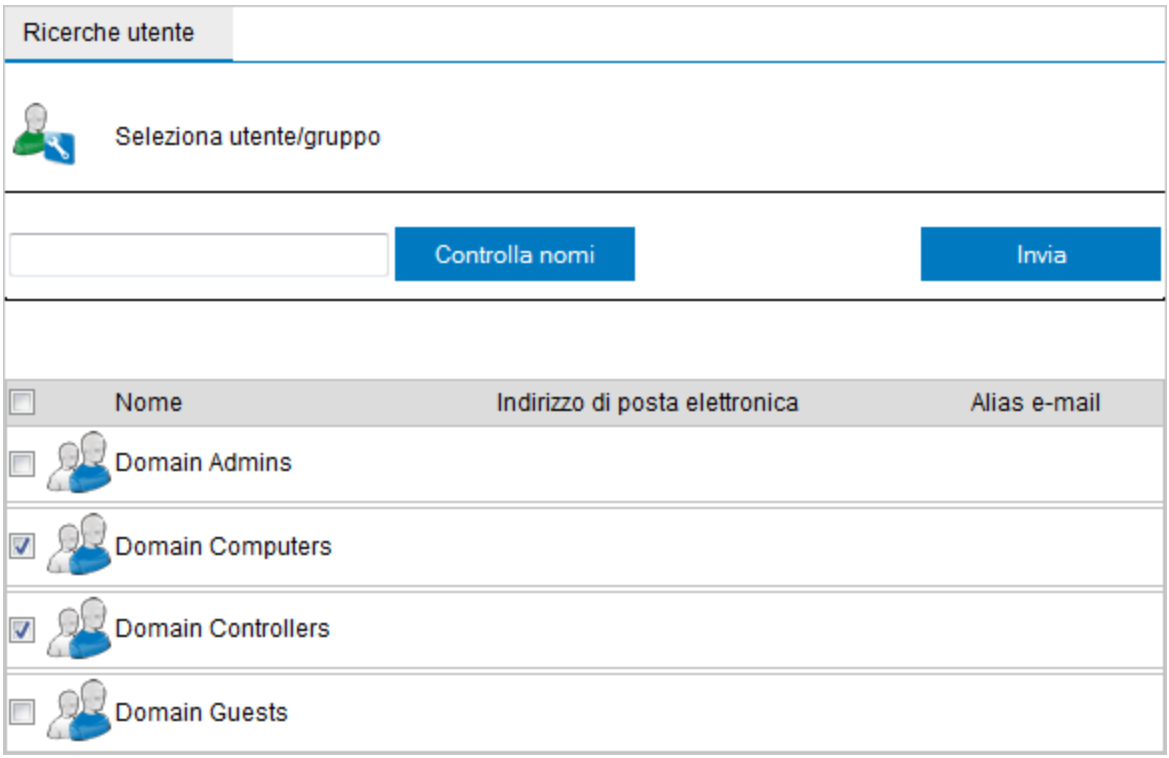


Schermata 102: Filtro contenuti: scheda Utenti/cartelle

2. Indicare gli utenti a cui applicare questa regola.

Opzione	Descrizione
Solo questo elenco	Applicare questa regola a un elenco personalizzato di utenti della posta, gruppi o cartelle pubbliche.
Tutto tranne questo elenco	Applicare questa regola a tutti gli utenti della posta, ad eccezione degli utenti, gruppi o cartelle pubbliche indicati in questo elenco.

3. Per aggiungere utenti della posta, gruppi di utenti e/o cartelle pubbliche all'elenco, fare clic su **Aggiungi**.



Schermata 103: Aggiunta di utenti a una regola di filtro dei contenuti

4. Nella finestra di dialogo **Ricerche utente**, inserire il nome dell'utente/gruppo di utenti di posta o della cartella pubblica da aggiungere, quindi fare clic su **Controlla nomi**. Di seguito verranno elencati i risultati trovati in utenti, gruppi o cartelle pubbliche.

> **NOTA**
> Non è necessario inserire il nome completo di utenti, gruppi o cartella pubblica. È sufficiente inserire una parte del nome. GFI MailEssentials elencherà tutti i nomi contenenti i caratteri specificati. Ad esempio, digitando `sco`, GFI MailEssentials verranno restituiti nomi come `Scott Adams` e `Freeman Prescott`, se disponibili.

5. Selezionare la casella di spunta accanto al nome da aggiungere all'elenco, quindi fare clic su **OK**.

> **NOTA**
> Per rimuovere le voci dall'elenco, selezionare l'utente/gruppo di utenti/cartella pubblica da rimuovere e fare clic su **Rimuovi**.

6. Ripetere i passaggi da 3 a 5 per aggiungere all'elenco tutti gli utenti necessari.

7. Fare clic su **Applica**.

7.2.2 Abilitazione/disabilitazione regole

Per abilitare (o disabilitare) le regole di filtro allegati:

1. Selezionare **Filtro contenuti > Filtro allegati**.

2. Dalla pagina **Filtro allegati**, selezionare la casella di controllo delle regole da abilitare o

disabilitare.

3. Di conseguenza, fare clic su **Abilita selezionati** o **Disabilita selezionati**.

7.2.3 Rimozione regole allegato

> **Avviso**
> Le regole eliminate non sono recuperabili. Nel dubbio, si consiglia di disabilitare una regola.

1. Selezionare **Filtro contenuti > Filtro allegati**.
2. Dalla pagina **Filtro allegati**, selezionare la regola da rimuovere.
3. Fare clic su **Rimuovi selezionati**.

7.2.4 Modifica di una regola esistente

1. Selezionare **Filtro contenuti > Filtro allegati**.
2. Dalla pagina **Filtro allegati**, fare clic sul nome della regola da modificare.
3. Eseguire le modifiche richieste nelle proprietà della regola, quindi fare clic su **Applica**.

7.2.5 Modifica priorità regola

Le regole del Filtro allegati vengono applicate nel medesimo ordine, dall'inizio alla fine nel modo in cui sono elencate nella pagina Filtro allegati (ovvero, viene controllata per prima una regola con il valore di priorità 1). Per modificare la sequenza/priorità delle regole:

1. Selezionare **Filtro contenuti > Filtro allegati**.
2. Dalla pagina Filtro allegati, fare clic sulle frecce ↑ (su) o ↓ (giù) per aumentare o diminuire rispettivamente la priorità della regola.
3. Ripetere il passaggio 2 finché le regole non sono collocate nella sequenza desiderata.

7.3 Filtro avanzato contenuto

Filtro avanzato contenuto consente la scansione dei dati e del contenuto dell'intestazione del messaggio, ricorrendo a condizioni di ricerca ed espressioni regolari configurabili (regex).

Per configurare le regole avanzate dei contenuti, selezionare **Filtro contenuti > Filtro avanzato contenuto**. Questa pagina consente all'utente di visualizzare, creare, abilitare, disabilitare o eliminare le regole.

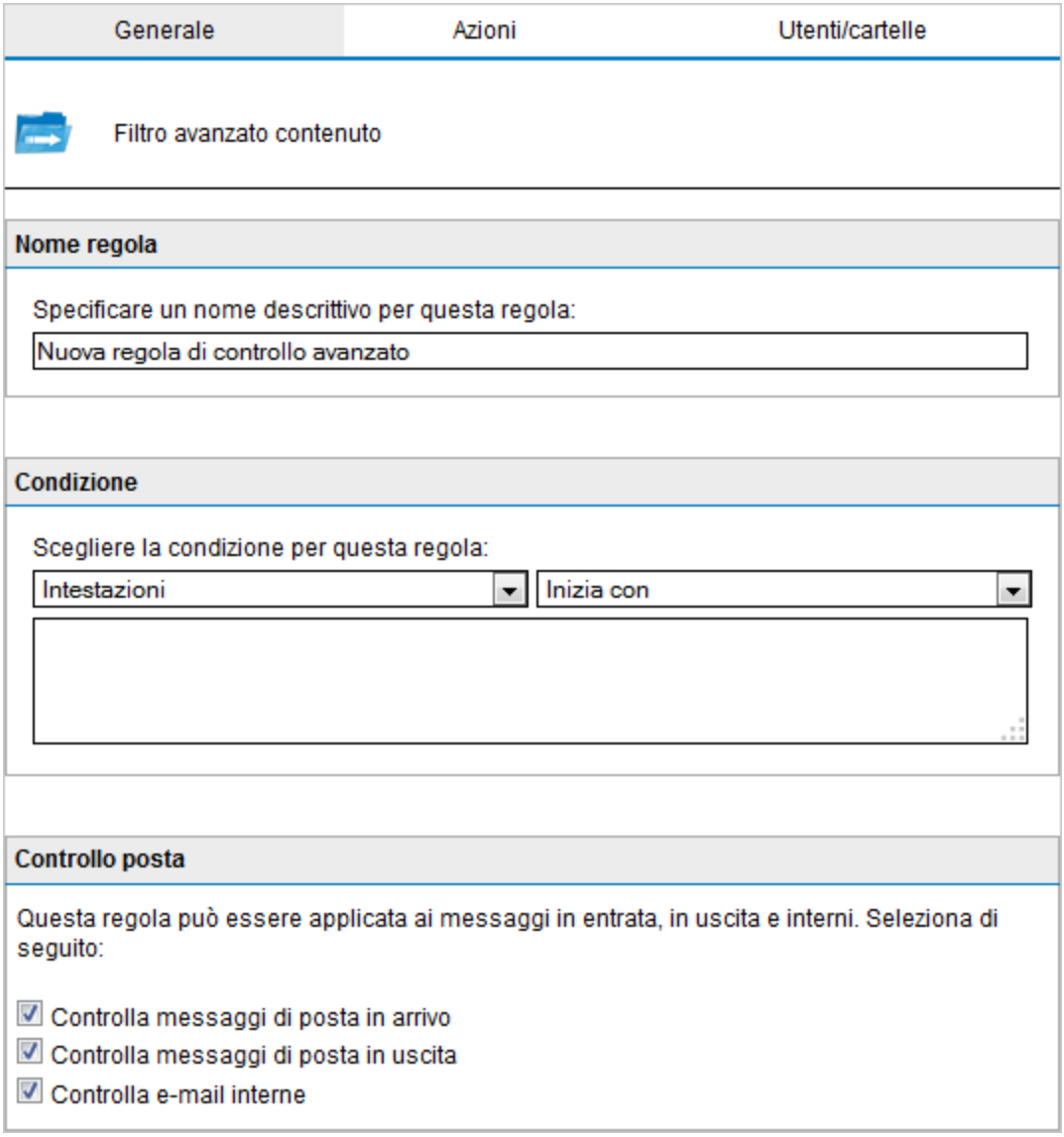
7.3.1 Creazione regole filtro avanzato contenuto

Per creare una regola di Filtro avanzato contenuto, attenersi ai passaggi elencati di seguito:

- » Passaggio 1: configurazione delle impostazioni di base delle regole e condizioni da bloccare
- » Passaggio 2: configurazione delle azioni da intraprendere sui messaggi rilevati
- » Passaggio 3: indicazione degli utenti a cui applicare questa regola

Passaggio 1: configurazione delle impostazioni di base delle regole e condizioni da bloccare

1. Selezionare **Filtro contenuti > Filtro avanzato contenuto** e fare clic su **Aggiungi regola...**



Schermata 104: aggiunta di una nuova regola di filtro avanzato contenuto

2. In **Nome regola**, digitare un nome per la nuova regola.

3. Nell'area **Condizione**, indicare la condizione che il messaggio deve soddisfare per rispettare questa regola. Dall'elenco a discesa selezionare la parte del messaggio (**Intestazione**, **Oggetto**, **Corpo**, **Nome allegato** o **Contenuto allegato**) e scegliere la condizione (**Inizia con**, **Termina con**, **Contiene**, **Corrispondenza perfetta**, **Corrisponde a Regex**). Nella casella di testo, immettere la parola chiave o l'espressione regolare che deve essere contenuta nel messaggio.

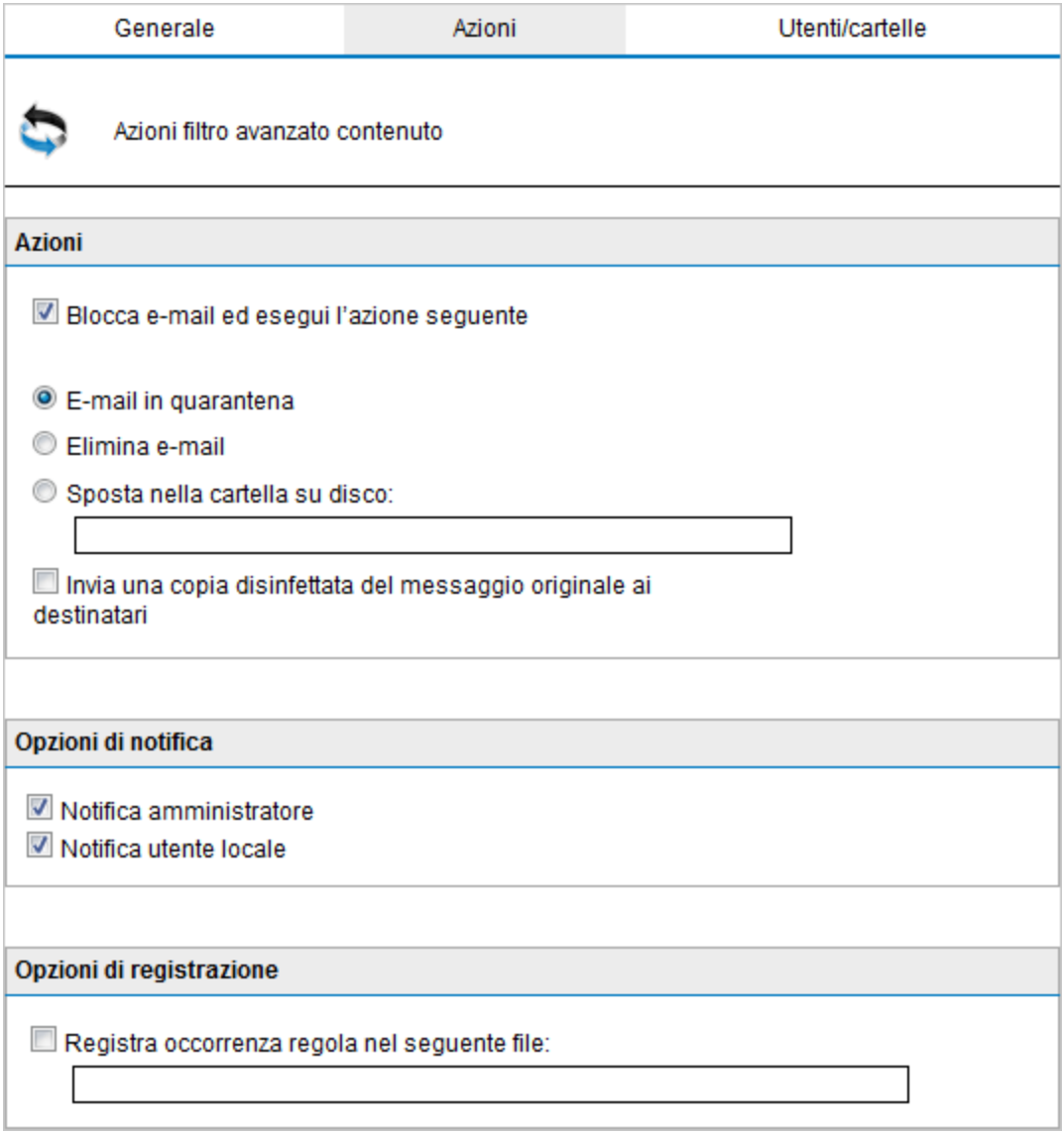
> **Ad esempio**: per associare i messaggi con `svizzero` nell'oggetto - Selezionare **Oggetto** e **Contiene**, quindi digitare `svizzero` nella casella di testo.

4. Scegliere se scansionare i messaggi in entrata, in uscita e/o interni.

Opzione	Descrizione
Controlla messaggi di posta in arrivo	Selezionare l'opzione per scansionare i messaggi in entrata.
Controlla messaggi di posta in uscita	Selezionare l'opzione per scansionare i messaggi in uscita.
Controlla e-mail interne	Selezionare questa opzione per scansionare i messaggi interni. **NOTA** Questa opzione è disponibile solo quando GFI MailEssentials è installato in un computer Microsoft® Exchange Server.

Passaggio 2: configurazione delle azioni da intraprendere sui messaggi rilevati

1. Dalla scheda **Azioni**, configurare quello che accade quando si attiva questa regola.



Schermata 105: scheda Azioni

2. Per bloccare un messaggio che rispetta le condizioni della regola, selezionare **Blocca e-mail ed esegui l'azione seguente**, quindi fare clic su una delle seguenti opzioni:

Opzione	Descrizione
E-mail in quarantena	Archivia i messaggi bloccati in Quarantine Store. I messaggi inseriti in quarantena potranno essere successivamente rivisti (per approvazione/eliminazione). Per ulteriori informazioni, fare riferimento a Quarantena (pagina 203).
Elimina e-mail	Elimina i messaggi di posta bloccati.
Sposta nella cartella su disco	Sposta il messaggio in una cartella su disco. Digitare il percorso completo della cartella dove salvare i messaggi bloccati.

IMPORTANTE

Le azioni interessano sempre l'intero messaggio il cui contenuto è bloccato, anche in presenza di altro contenuto (come gli allegati) che non attiva questa regola.

NOTA

Quando GFI MailEssentials viene installato sullo stesso computer di Microsoft® Exchange 2003, GFI MailEssentials potrebbe non riuscire a bloccare i messaggi in uscita ma invece sostituire il contenuto bloccato con un rapporto sulle minacce.

3. Selezionare **Invia una copia disinfettata del messaggio originale ai destinatari** per scegliere se inviare ai destinatari una copia del messaggio bloccato, privo dei contenuti dannosi.

4. GFI MailEssentials può inviare notifiche di posta ogni volta che un messaggio attiva questo filtro. Per abilitare questa funzione, selezionare una delle seguenti opzioni:

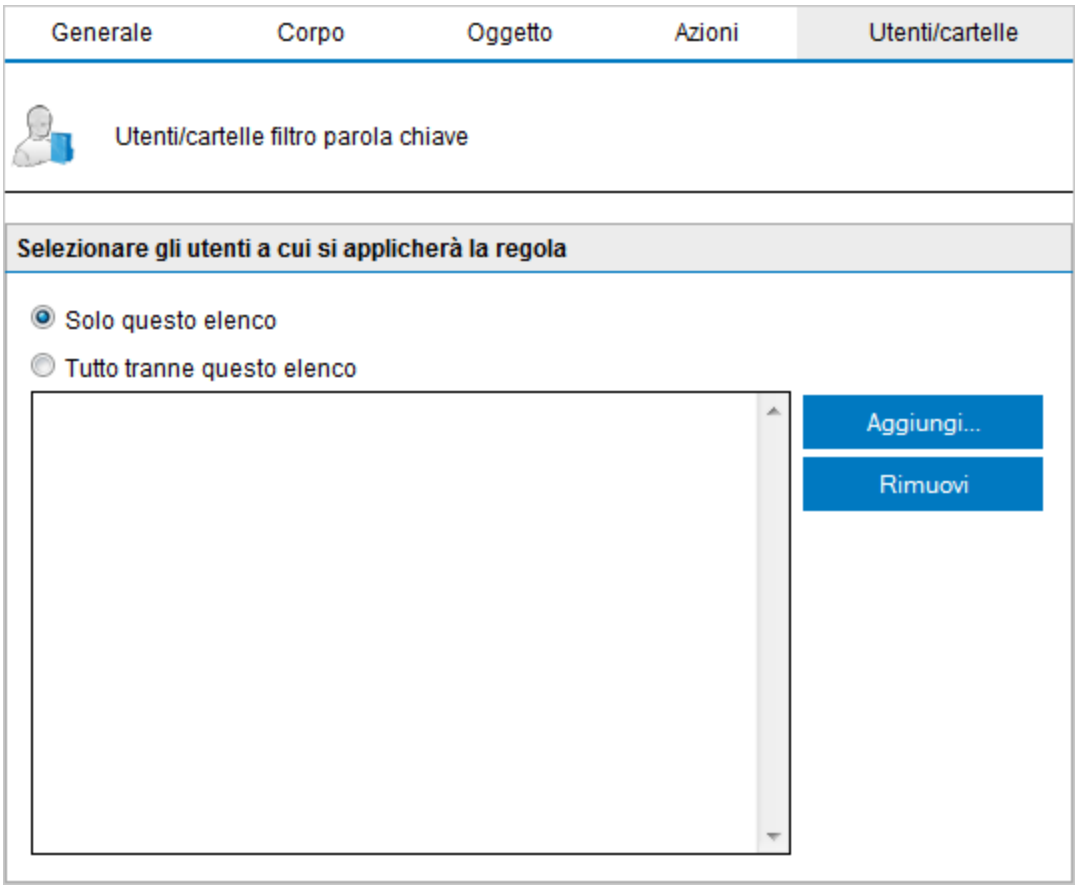
Opzione	Descrizione
Notifica amministratore	Notifica l'amministratore quando questo motore blocca un messaggio. Per ulteriori informazioni, fare riferimento a Indirizzo e-mail amministratore (pagina 241).
Notifica utente locale	Notifica il messaggio bloccato ai destinatari locali del messaggio.

5. Per registrare l'attività di questo motore in un file di registro, selezionare **Registra occorrenze nel seguente file**. Nella casella di testo, indicare il percorso e il nome del file di una posizione personalizzata su disco dove è possibile salvare il file di registro. Per impostazione predefinita, i file di registro vengono archiviati in:

```
<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\EmailSecurity\Logs\<nome motore>.log
```

Passaggio 3: indicazione degli utenti a cui applicare questa regola

1. Per impostazione predefinita, questa regola viene applicata a tutti gli utenti della posta. Tuttavia, GFI MailEssentials permette di applicare questa regola a un elenco personalizzato di utenti della posta indicati nella scheda Utenti/Cartelle.

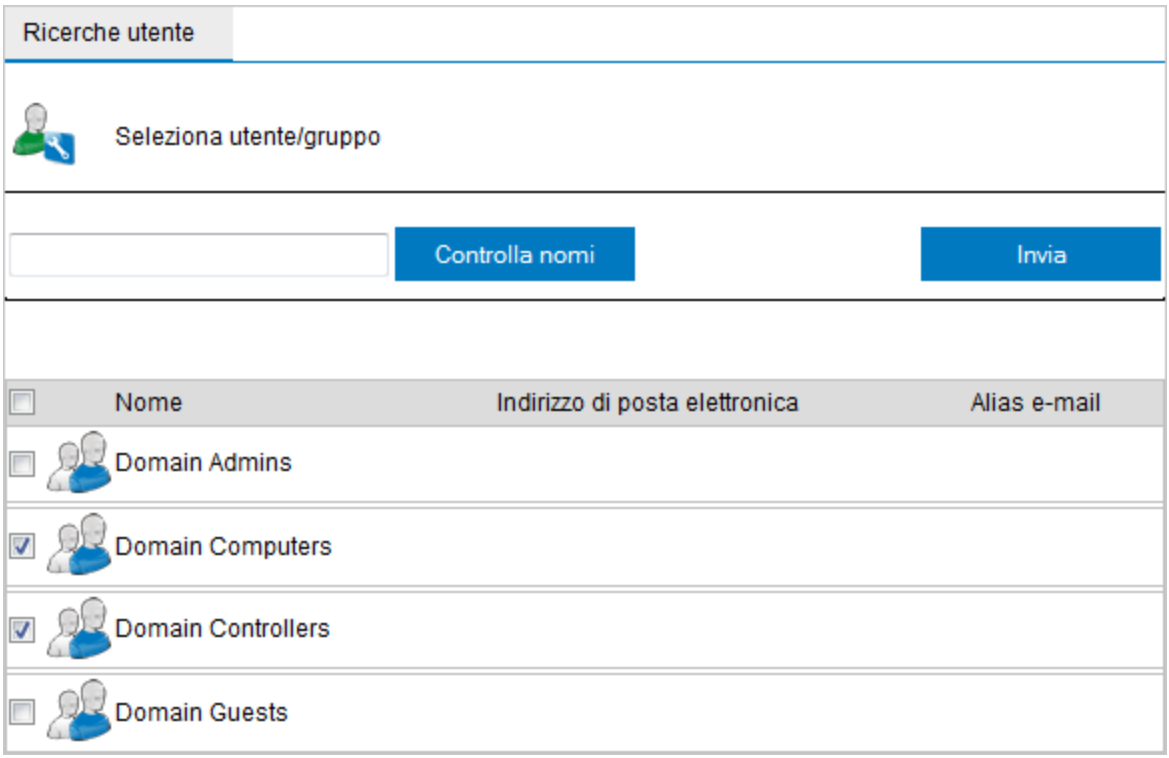


Schermata 106: Filtro contenuti: scheda Utenti/cartelle

2. Indicare gli utenti a cui applicare questa regola.

Opzione	Descrizione
Solo questo elenco	Applicare questa regola a un elenco personalizzato di utenti della posta, gruppi o cartelle pubbliche.
Tutto tranne questo elenco	Applicare questa regola a tutti gli utenti della posta, ad eccezione degli utenti, gruppi o cartelle pubbliche indicati in questo elenco.

3. Per aggiungere utenti della posta, gruppi di utenti e/o cartelle pubbliche all'elenco, fare clic su **Aggiungi**.



Schermata 107: Aggiunta di utenti a una regola di filtro dei contenuti

4. Nella finestra di dialogo **Ricerche utente**, inserire il nome dell'utente/gruppo di utenti di posta o della cartella pubblica da aggiungere, quindi fare clic su **Controlla nomi**. Di seguito verranno elencati i risultati trovati in utenti, gruppi o cartelle pubbliche.

> **NOTA**
> Non è necessario inserire il nome completo di utenti, gruppi o cartella pubblica. È sufficiente inserire una parte del nome. GFI MailEssentials elencherà tutti i nomi contenenti i caratteri specificati. Ad esempio, digitando `sco`, GFI MailEssentials verranno restituiti nomi come `Scott Adams` e `Freeman Prescott`, se disponibili.

5. Selezionare la casella di spunta accanto al nome da aggiungere all'elenco, quindi fare clic su **OK**.

> **NOTA**
> Per rimuovere le voci dall'elenco, selezionare l'utente/gruppo di utenti/cartella pubblica da rimuovere e fare clic su **Rimuovi**.

6. Ripetere i passaggi da 3 a 5 per aggiungere all'elenco tutti gli utenti necessari.

7. Fare clic su **Applica**.

7.3.2 Rimozione regole

1. Da **Filtro contenuti > Filtro avanzato contenuto**, selezionare la regola da rimuovere.

2. Fare clic su **Rimuovi selezionati**.

7.3.3 Abilitazione/disabilitazione regole

1. Da **Filtro contenuti > Filtro avanzato contenuto**, selezionare la regola da abilitare/disabilitare.

2. Fare clic su **Disabilita selezionati** per disabilitare la regola o su **Abilita selezionati** per abilitarla.

7.3.4 Regole di ordinamento

Le regole del Filtro avanzato contenuto vengono applicate nel medesimo ordine, dall'inizio alla fine nel modo in cui sono elencate nella pagina Filtro avanzato contenuto (ovvero, viene controllata per prima una regola con il valore di priorità 1). Per modificare la sequenza/priorità delle regole:

1. Selezionare **Filtro contenuti > nodo Filtro avanzato contenuto**.

2. Fare clic sulle frecce (su) o (giù) per aumentare o diminuire rispettivamente la priorità della regola.

3. Ripetere il passaggio 2 finché le regole non sono collocate nella sequenza desiderata.

7.4 Motore di decompressione

Motore di decompressione estrae e analizza gli archivi (file compressi) allegati a un messaggio.

Di seguito, un elenco di controlli effettuati dal motore di decompressione:

- Archivi protetti da password
- Archivi danneggiati
- Archivi ricorsivi
- Dimensione file decompressi negli archivi
- Dimensioni file negli archivi
- Scansiona negli archivi

7.4.1 Configurazione motori di decompressione filtri

Per configurare i filtri del motore di decompressione:

1. Selezionare **Filtro contenuti > nodo Decompressione**.

Schermata 108: controlli motore di decompressione

2. Fare clic sul filtro di decompressione per configurare:

» Controlla archivi protetti da password

» Controlla archivi danneggiati

» Controlla archivi ricorsivi

» Controlla dimensione file non compressi negli archivi

» Controlla numero di file negli archivi

» Scansiona negli archivi

Controlla archivi protetti da password

1. Selezionare **Filtro contenuti > nodo Decompressione**.

2. Dall'elenco dei filtri disponibili, fare clic su **Controlla archivi protetti da password**.

3. Per abilitare questo filtro, selezionare **Controlla archivi protetti da password**.

4. Specificare l'operazione da eseguire quando un messaggio contiene un archivio che attiva questo filtro:

Opzione	Descrizione
Quarantena	Inserisce in quarantena i messaggi bloccati.
Elimina automaticamente	Elimina i messaggi di posta bloccati.

NOTA
Quando GFI MailEssentials viene installato sullo stesso computer di Microsoft® Exchange 2003, GFI MailEssentials potrebbe non riuscire a bloccare i messaggi in uscita ma invece sostituire il contenuto bloccato con un rapporto sulle minacce.

5. Selezionare **Invia una copia disinfettata del messaggio originale ai destinatari** per scegliere se inviare ai destinatari una copia del messaggio bloccato.

6. Per configurare le azioni successive, fare clic sulla scheda **Azioni**.

7. GFI MailEssentials può inviare notifiche di posta ogni volta che un messaggio attiva questo filtro. Per abilitare questa funzione, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Notifica amministratore	Notifica l'amministratore quando questo motore blocca un messaggio. Per ulteriori informazioni, fare riferimento a Indirizzo e-mail amministratore (pagina 241).
Notifica utente locale	Notifica il messaggio bloccato ai destinatari locali del messaggio.

8. Per registrare l'attività di questo motore in un file di registro, selezionare **Registra occorrenze nel seguente file**. Nella casella di testo, indicare il percorso e il nome del file di una posizione personalizzata su disco dove è possibile salvare il file di registro. Per impostazione predefinita, i file di registro vengono archiviati in:

```
<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\EmailSecurity\Logs\<nome motore>.log
```

9. Fare clic su **Applica**.

Controlla archivi danneggiati

1. Selezionare **Filtro contenuti > nodo Decompressione**.

2. Dall'elenco dei filtri disponibili, fare clic su **Controlla archivi danneggiati**.

3. Per abilitare questo filtro, selezionare **Controlla archivi danneggiati**.

4. Specificare l'operazione da eseguire quando un messaggio contiene un archivio che attiva questo filtro:

Opzione	Descrizione
Quarantena	Inserisce in quarantena i messaggi bloccati.
Elimina automaticamente	Elimina i messaggi di posta bloccati.

NOTA
Quando GFI MailEssentials viene installato sullo stesso computer di Microsoft® Exchange 2003, GFI MailEssentials potrebbe non riuscire a bloccare i messaggi in uscita ma invece sostituire il contenuto bloccato con un rapporto sulle minacce.

5. Selezionare **Invia una copia disinfettata del messaggio originale ai destinatari** per scegliere se inviare ai destinatari una copia del messaggio bloccato.

6. Per configurare le azioni successive, fare clic sulla scheda **Azioni**.

7. GFI MailEssentials può inviare notifiche di posta ogni volta che un messaggio attiva questo filtro. Per abilitare questa funzione, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Notifica amministratore	Notifica l'amministratore quando questo motore blocca un messaggio. Per ulteriori informazioni, fare riferimento a Indirizzo e-mail amministratore (pagina 241).
Notifica utente locale	Notifica il messaggio bloccato ai destinatari locali del messaggio.

8. Per registrare l'attività di questo motore in un file di registro, selezionare **Registra occorrenze nel seguente file**. Nella casella di testo, indicare il percorso e il nome del file di una posizione personalizzata su disco dove è possibile salvare il file di registro. Per impostazione predefinita, i file di registro vengono archiviati in:

```
<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\EmailSecurity\Logs\<nome motore>.log
```

9. Fare clic su **Applica**.

Controlla archivi ricorsivi

Questo filtro consente di inserire in quarantena o eliminare i messaggi che contengono archivi ricorsivi. Gli archivi ricorsivi, noti anche come archivi nidificati, sono archivi che contengono livelli multipli di archivi secondari (archivi contenuti all'interno di altri). Un numero elevato di livelli di archivio può indicare un archivio dannoso. Gli archivi ricorsivi possono essere utilizzati in un attacco DoS (Denial of Service), poiché consumano risorse dei computer durante l'analisi. Per configurare questo filtro:

1. Selezionare **Filtro contenuti > nodo Decompressione**.

2. Dall'elenco dei filtri disponibili, fare clic su **Controlla archivi ricorsivi**.

3. Per abilitare questo filtro, selezionare **Controlla archivi ricorsivi**.

4. Specificare il numero massimo di archivi ricorsivi nella casella di testo **Numero massimo archivi ricorrenti**. Se un archivio contiene più archivi ricorsivi del numero indicato, il messaggio viene classificato come dannoso.

5. Specificare l'operazione da eseguire quando un messaggio contiene un archivio che attiva questo filtro:

Opzione	Descrizione
Quarantena	Inserisce in quarantena i messaggi bloccati.
Elimina automaticamente	Elimina i messaggi di posta bloccati.

> **NOTA**
> Quando GFI MailEssentials viene installato sullo stesso computer di Microsoft® Exchange 2003, GFI MailEssentials potrebbe non riuscire a bloccare i messaggi in uscita ma invece sostituire il contenuto bloccato con un rapporto sulle minacce.

6. Selezionare **Invia una copia disinfettata del messaggio originale ai destinatari** per scegliere se inoltrare ai destinatari una copia del messaggio bloccato, privo dei contenuti dannosi.

7. Per configurare le azioni successive, fare clic sulla scheda **Azioni**.

8. GFI MailEssentials può inviare notifiche di posta ogni volta che un messaggio attiva questo filtro. Per abilitare questa funzione, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Notifica amministratore	Notifica l'amministratore quando questo motore blocca un messaggio. Per ulteriori informazioni, fare riferimento a Indirizzo e-mail amministratore (pagina 241).
Notifica utente locale	Notifica il messaggio bloccato ai destinatari locali del messaggio.

9. Per registrare l'attività di questo motore in un file di registro, selezionare **Registra occorrenze nel seguente file**. Nella casella di testo, indicare il percorso e il nome del file di una posizione personalizzata su disco dove è possibile salvare il file di registro. Per impostazione predefinita, i file di registro vengono archiviati in:

```
<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\EmailSecurity\Logs\<nome motore>.log
```

10. Fare clic su **Applica**.

Controlla dimensione file non compressi negli archivi

Questo filtro consente di bloccare o eliminare i messaggi i cui archivi superano le dimensioni fisiche specificate, quando non sono compressi. A volte gli hacker adottano questo metodo nell'attacco DoS (Denial of Service), eseguendo l'invio di un archivio che può essere decompresso diventando un file molto grande, consumando spazio su disco e richiedendo molto tempo per l'analisi da parte di software di sicurezza dei contenuti o antivirus.

Per configurare questo filtro:

1. Selezionare **Filtro contenuti > nodo Decompressione**.

2. Dall'elenco dei filtri disponibili, fare clic su **Controlla dimensione file non compressi negli archivi**.

3. Per abilitare questo filtro, selezionare **Controlla dimensione file non compressi negli archivi**.

4. Specificare il numero massimo di archivi non compressi nella casella di testo **Dimensione massima file non compressi in MB**. Se le dimensioni di un archivio non compresso sono superiori al valore specificato, il messaggio viene classificato come dannoso.

5. Specificare l'operazione da eseguire quando un messaggio contiene un archivio che attiva questo filtro:

Opzione	Descrizione
Quarantena	Inserisce in quarantena i messaggi bloccati.
Elimina automaticamente	Elimina i messaggi di posta bloccati.

NOTA

Quando GFI MailEssentials viene installato sullo stesso computer di Microsoft® Exchange 2003, GFI MailEssentials potrebbe non riuscire a bloccare i messaggi in uscita ma invece sostituire il contenuto bloccato con un rapporto sulle minacce.

6. Selezionare **Invia una copia disinfettata del messaggio originale ai destinatari** per scegliere se inviare ai destinatari una copia del messaggio bloccato, privo dei contenuti dannosi.

7. GFI MailEssentials può inviare notifiche di posta ogni volta che un messaggio attiva questo filtro. Per abilitare questa funzione, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Notifica amministratore	Notifica l'amministratore quando questo motore blocca un messaggio. Per ulteriori informazioni, fare riferimento a Indirizzo e-mail amministratore (pagina 241).
Notifica utente locale	Notifica il messaggio bloccato ai destinatari locali del messaggio.

8. Per registrare l'attività di questo motore in un file di registro, selezionare **Registra occorrenze nel seguente file**. Nella casella di testo, indicare il percorso e il nome del file di una posizione personalizzata su disco dove è possibile salvare il file di registro. Per impostazione predefinita, i file di registro vengono archiviati in:

```
<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\EmailSecurity\Logs\<nome motore>.log
```

9. Fare clic su **Applica**.

Controlla numero di file negli archivi

Questo filtro consente di inserire in quarantena o eliminare i messaggi che contengono un numero eccessivo di file compressi all'interno di un archivio allegato. È possibile specificare il numero di file consentiti negli allegati dall'archivio dalle opzioni di configurazione incluse nel filtro. Per configurare questo filtro:

1. Selezionare **Filtro contenuti > nodo Decompressione**.

2. Dall'elenco dei filtri disponibili, fare clic su **Controlla numero di file negli archivi**.

3. Per abilitare questo filtro, selezionare **Controlla numero di file negli archivi**.

4. Specificare il numero massimo di file negli archivi nella casella di testo **Se il numero di file all'interno dell'archivio supera**. Se un archivio contiene più file del valore specificato, il messaggio viene classificato come dannoso.

5. Specificare l'operazione da eseguire quando un messaggio contiene un archivio che attiva questo filtro:

Opzione	Descrizione
Quarantena	Inserisce in quarantena i messaggi bloccati.
Elimina automaticamente	Elimina i messaggi di posta bloccati.

NOTA
Quando GFI MailEssentials viene installato sullo stesso computer di Microsoft® Exchange 2003, GFI MailEssentials potrebbe non riuscire a bloccare i messaggi in uscita ma invece sostituire il contenuto bloccato con un rapporto sulle minacce.

6. Selezionare **Invia una copia disinfettata del messaggio originale ai destinatari** per scegliere se inviare ai destinatari una copia del messaggio bloccato.

7. Per configurare le azioni successive, fare clic sulla scheda **Azioni**.

8. GFI MailEssentials può inviare notifiche di posta ogni volta che un messaggio attiva questo filtro. Per abilitare questa funzione, selezionare una delle seguenti opzioni:

Opzione	Descrizione
Notifica amministratore	Notifica l'amministratore quando questo motore blocca un messaggio. Per ulteriori informazioni, fare riferimento a Indirizzo e-mail amministratore (pagina 241).
Notifica utente locale	Notifica il messaggio bloccato ai destinatari locali del messaggio.

9. Per registrare l'attività di questo motore in un file di registro, selezionare **Registra occorrenze nel seguente file**. Nella casella di testo, indicare il percorso e il nome del file di una posizione personalizzata su disco dove è possibile salvare il file di registro. Per impostazione predefinita, i file di registro vengono archiviati in:

```
<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\EmailSecurity\Logs\<nome motore>.log
```

10. Fare clic su **Applica**.

Scansiona negli archivi

È possibile configurare GFI MailEssentials affinché applichi il filtro allegati e parole chiave ai file contenuti all'interno degli archivi.

1. Selezionare **Filtro contenuti > nodo Decompressione**.

2. Dall'elenco di filtri disponibili, fare clic su **Scansiona negli archivi**.

3. Per abilitare la scansione all'interno degli archivi, selezionare **Applica regole di filtro allegati e contenuti agli archivi**. Per ulteriori informazioni, fare riferimento a Filtro contenuti (pagina 176).

4. Fare clic su **Applica**.

7.4.2 Abilitazione/disabilitaziona filtri di decompressione

Per abilitare (o disabilitare) i filtri di decompressione:

1. Selezionare **Filtro contenuti > nodo Decompressione**.

2. Dalla pagina **Motore di decompressione**, selezionare la casella di controllo delle regole da abilitare o disabilitare.

3. Di conseguenza, fare clic su **Abilita selezionati** o **Disabilita selezionati**.

8 Quarantena

La funzionalità di quarantena di GFI MailEssentials fornisce un archivio centrale dove tutta la posta rilevata come spam o malware viene conservata. In tal modo si assicura che gli utenti non ricevano posta indesiderata e malware nella loro cassetta postale, riducendo al contempo l'elaborazione da parte del server della posta.

Gli amministratori e gli utenti della posta possono rivedere i messaggi in quarantena accedendo all'interfaccia della quarantena da un browser Web. GFI MailEssentials può anche inviare dei rapporti e-mail regolari agli utenti della posta per rivedere i loro messaggi bloccati.

Per ulteriori informazioni sulla configurazione della quarantena di GFI MailEssentials, fare riferimento alle seguenti sezioni.

8.1 Note importanti **203**

8.2 Ricerca nella quarantena **203**

8.3 Cartelle ricerche **209**

8.4 Operazioni con i messaggi messi in quarantena **213**

8.5 Feed RSS quarantena **216**

8.6 Opzioni quarantena **218**

8.7 Percorso e URL pubblico di Quarantine Store **225**

8.1 Note importanti

1. Per mettere in quarantena lo spam o i messaggi dannosi, impostare le azioni dei filtri e dei motori su **E-mail in quarantena**.

2. Quarantine Store richiede spazio su disco per conservare le e-mail di spam o malware dell'organizzazione per alcuni giorni. La quantità di spazio su disco richiesto dipende da:

- la quantità ricevuta
- la durata della conservazione

3. In media, 100.000 messaggi spam o malware di 5 KB ciascuno richiederanno circa 600 MB di spazio su disco per l'archiviazione del messaggio e dei relativi metadati.

4. Se lo spazio disponibile sul disco dove si trova Quarantine Store è di 512 MB o meno, GFI MailEssentials interromperà la messa in quarantena dello spam, che invece verrà contrassegnata e recapitata nelle cassette postali dei destinatari finché la quantità di spazio libero sul disco non sarà superiore a 512 MB. In tal modo si garantisce che il disco non esaurisca lo spazio.

8.2 Ricerca nella quarantena

Quarantine Store è accessibile dall'interfaccia di GFI MailEssentials e consente la gestione dei messaggi inseriti in quarantena.

Per accedere a GFI MailEssentials Quarantine Store, selezionare **GFI MailEssentials > Quarantena**.

Esistono vari modi di cercare il contenuto nella quarantena di GFI MailEssentials:

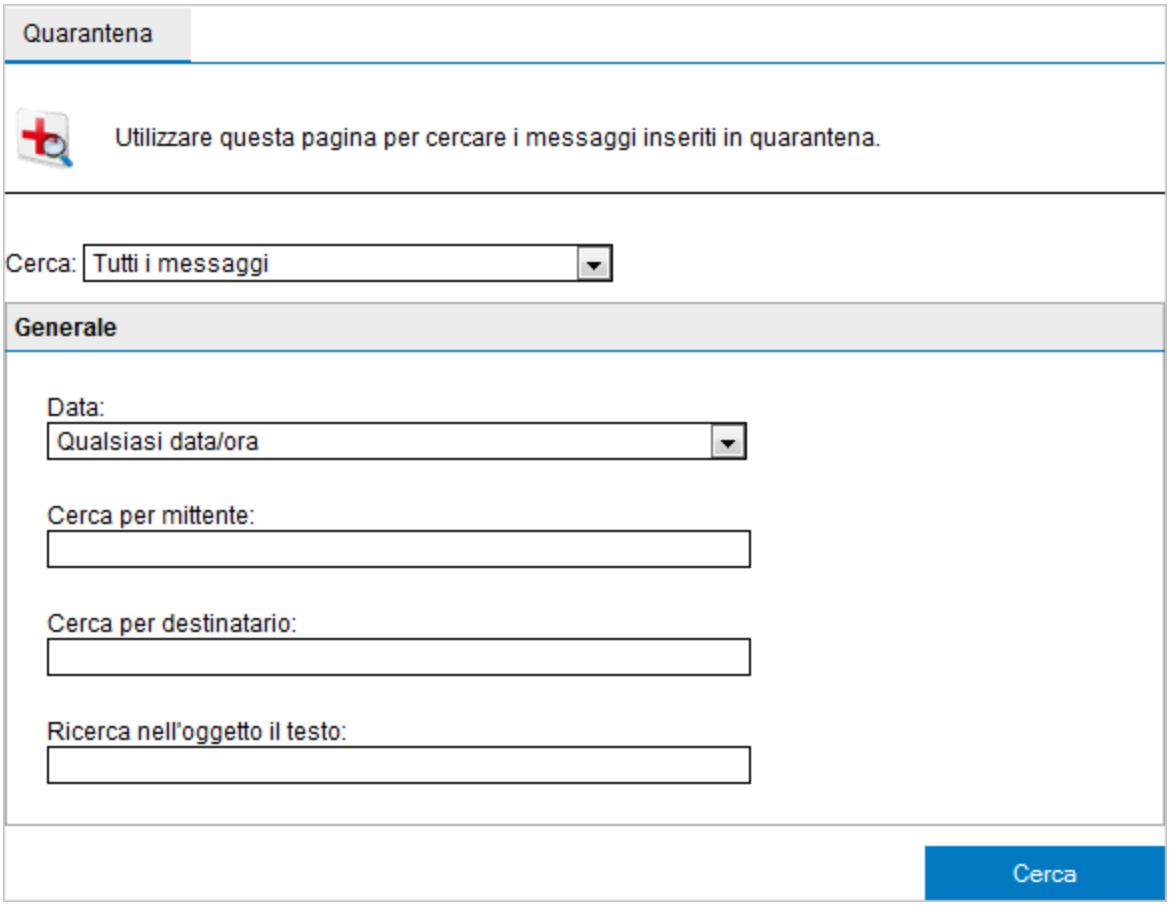
» Ricerca nel malware e spam inserito in quarantena

» Ricerca solo nei messaggi malware

» Ricerca solo nei messaggi spam

Ricerca di malware e spam

1. Selezionare **GFI MailEssentials > Quarantena**.



Schermata 109: area di ricerca di malware e spam

2. Dalla pagina **Quarantena**, selezionare **Tutti i messaggi** dall'elenco **Cerca**.

3. Specificare i criteri di ricerca richiesti.

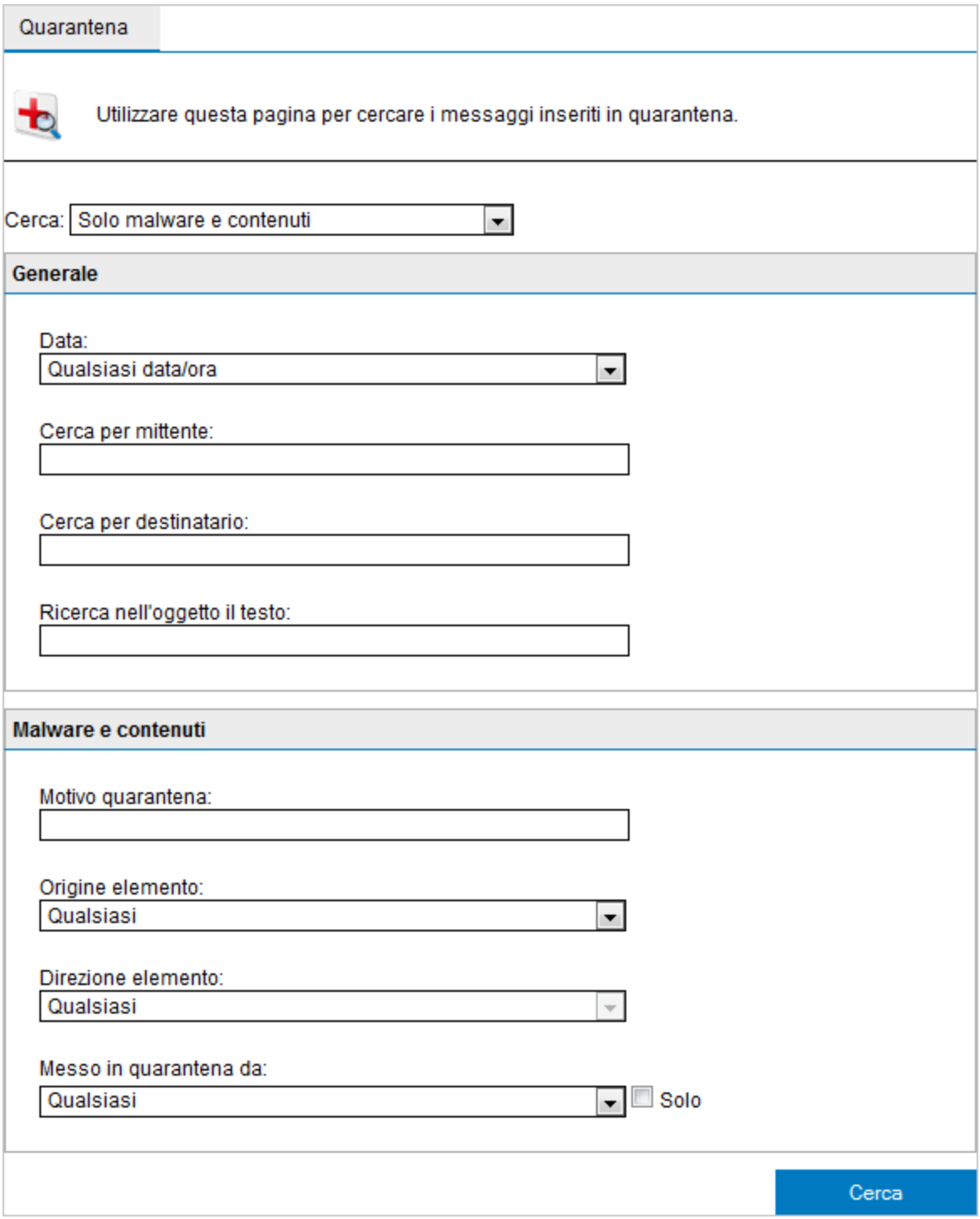
CRITERI DI RICERCA	DESCRIZIONE
Data:	Selezionare l'intervallo di date in cui il messaggio è stato inserito in quarantena. Gli intervalli date disponibili sono: » Qualsiasi data/ora » Da ieri » Ultimi 7 giorni » Ultimi 30 giorni » Intervallo di date personalizzato
Cerca per mittente	Indicare un mittente che ha inviato il messaggio inserito in quarantena.
Cerca per destinatario	Indicare un destinatario di cui è stato inserito in quarantena il messaggio.
Ricerca nell'oggetto il testo	Indicare il testo da cercare nell'oggetto del messaggio inserito in quarantena.

4. Fare clic su **Cerca**.

> **NOTA**
> Utilizza i risultati di ricerca per rivedere le e-mail in quarantena. È possibile approvare i falsi positivi per recapitarli ai destinatari. Per ulteriori informazioni, fare riferimento a Operazioni con i messaggi messi in quarantena (pagina 213).

Ricerca solo malware e contenuti

1. Selezionare **GFI MailEssentials > Quarantena**.



Schermata 110: area di ricerca di malware e spam

2. Dalla pagina **Quarantena**, selezionare **Solo malware e contenuti** dall'elenco a discesa **Cerca**.

3. Specificare i criteri di ricerca richiesti.

CRITERI DI RICERCA	DESCRIZIONE
Data:	Selezionare l'intervallo di date in cui il messaggio è stato inserito in quarantena. Gli intervalli date disponibili sono: » Qualsiasi data/ora » Da ieri » Ultimi 7 giorni » Ultimi 30 giorni » Intervallo di date personalizzato
Cerca per mittente	Indicare un mittente che ha inviato il messaggio inserito in quarantena.
Cerca per destinatario	Indicare un destinatario di cui è stato inserito in quarantena il messaggio.
Ricerca nell'oggetto il testo	Indicare il testo da cercare nell'oggetto del messaggio inserito in quarantena.
Motivo quarantena	Indicare il motivo per cui è stato inserito in quarantena il messaggio da cercare.
Origine elemento	Selezionare l'origine da cui è stato identificato il messaggio come malware e poi inserito in quarantena. Le opzioni disponibili sono: » Archivio informazioni (VSAPI) » Gateway (SMTP) » Archivio informazioni (trasporto)
Direzione elemento	Scegliere la direzione del messaggio inserito in quarantena da cercare. » Qualsiasi » In arrivo » In uscita **NOTA** Questa opzione è disponibile solo se **Gateway (SMTP)** è selezionato in **Origine elemento**.
Messo in quarantena da	Selezionare uno dei filtri di GFI MailEssentials che ha messo in quarantena il messaggio. Selezionare la casella di controllo **Solo** per cercare i messaggi inseriti in quarantena da un filtro specifico.

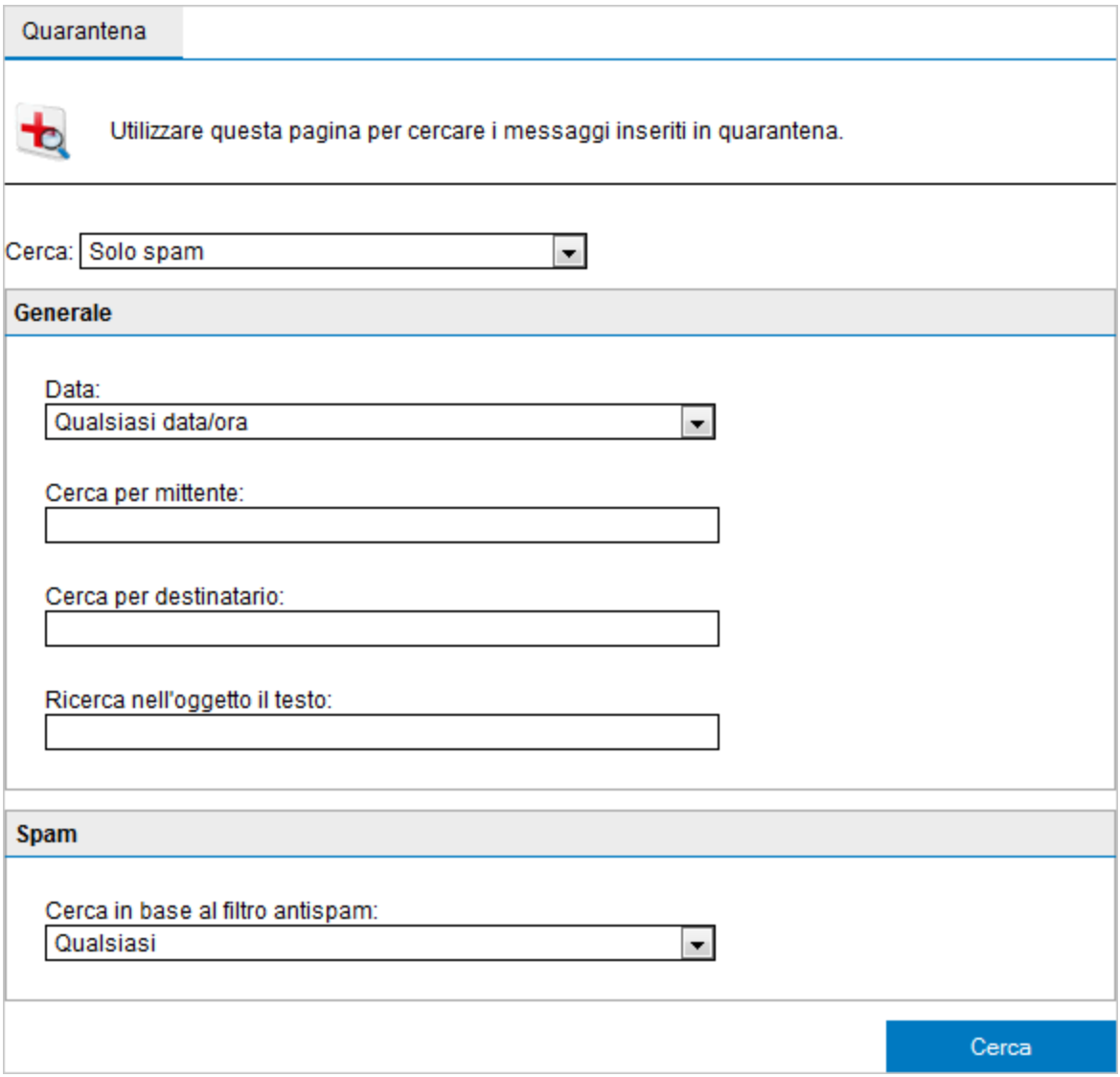
4. Fare clic su **Cerca**.

NOTA

Utilizza i risultati di ricerca per rivedere le e-mail in quarantena. È possibile approvare i falsi positivi per recapitarli ai destinatari. Per ulteriori informazioni, fare riferimento a Operazioni con i messaggi messi in quarantena (pagina 213).

Ricerca solo spam

1. Selezionare **GFI MailEssentials > Quarantena**.



Schermata 111: area di ricerca Solo spam

2. Dalla pagina **Quarantena**, selezionare **Solo spam** dall'elenco a discesa **Cerca**.

3. Specificare i criteri di ricerca richiesti. Le opzioni disponibili sono:

CRITERI DI RICERCA	DESCRIZIONE
Data:	Selezionare l'intervallo di date in cui il messaggio è stato inserito in quarantena. Gli intervalli date disponibili sono: » Qualsiasi data/ora » Da ieri » Ultimi 7 giorni » Ultimi 30 giorni » Intervallo di date personalizzato
Cerca per mittente	Indicare un mittente che ha inviato il messaggio inserito in quarantena.
Cerca per destinatario	Indicare un destinatario di cui è stato inserito in quarantena il messaggio.
Ricerca nell'oggetto il testo	Indicare il testo da cercare nell'oggetto del messaggio inserito in quarantena.
Cerca in base al filtro antispam	Scegliere il filtro antispam che ha identificato il messaggio per la ricerca spam.

4. Fare clic su **Cerca**.

> **NOTA**
> Utilizza i risultati di ricerca per rivedere le e-mail in quarantena. È possibile approvare i falsi positivi per recapitarli ai destinatari. Per ulteriori informazioni, fare riferimento a Operazioni con i messaggi messi in quarantena (pagina 213).

8.3 Cartelle ricerche

Una cartella di ricerca è una cartella con una query di ricerca personalizzata associata ad essa e mostra tutti i messaggi inseriti in quarantena che corrispondono a tale query.

Esempi di cartelle di ricerca:

» Una cartella di ricerca che mostra solo i messaggi in uscita inseriti in quarantena dai motori di scansione antivirus.

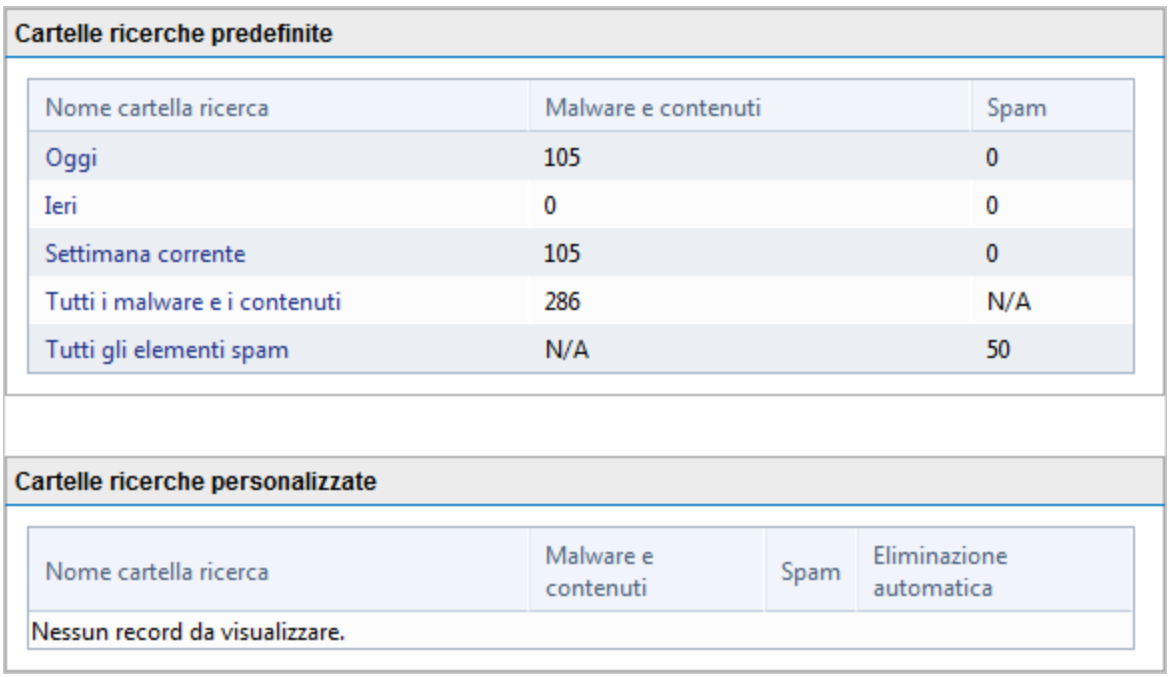
» Una cartella di ricerca che mostra i messaggi in entrata inseriti in quarantena in un determinato intervallo di date e indirizzati a un utente specifico.

» Una cartella di ricerca che mostra i messaggi che soddisfano criteri di ricerca specifici.

» Una cartella di ricerca che mostra i risultati di una query di ricerca precedentemente definita.

Per visualizzare i messaggi in una cartella di ricerca specifica:

1. Selezionare il nodo **Quarantena**.



Schermata 112: cartelle di ricerca personalizzate e predefinite

2. Fare clic su una cartella di ricerca visualizzata nelle aree **Cartelle ricerche predefinite** o **Cartelle ricerche personalizzate**. In alternativa, selezionare uno dei nodi della cartella di ricerca accessibili da **Quarantena** e dal nodo **Quarantena > Cartelle ricerche**.

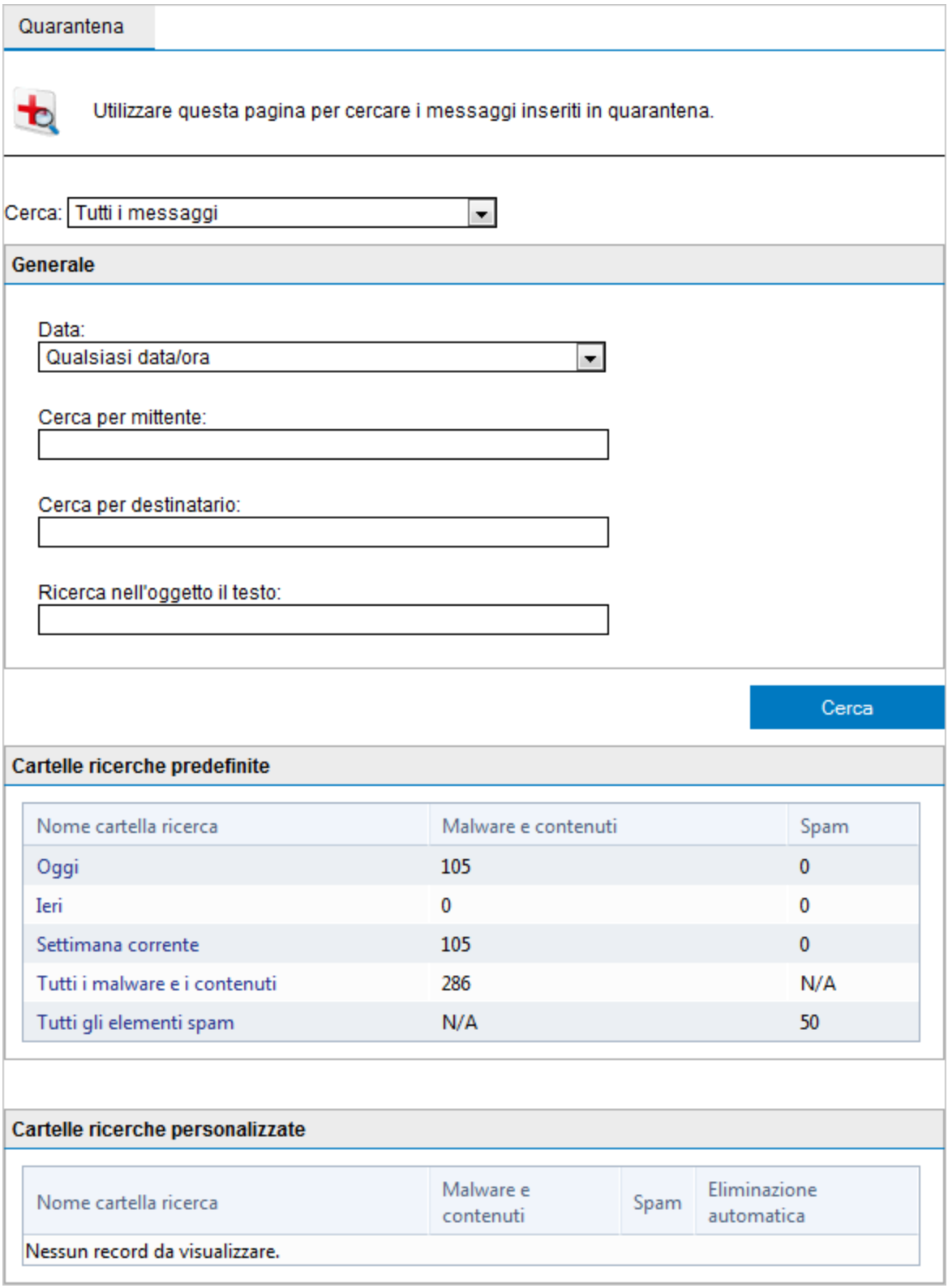
NOTA

Utilizza i risultati di ricerca per rivedere le e-mail in quarantena. È possibile approvare i falsi positivi per recapitarli ai destinatari. Per ulteriori informazioni, fare riferimento a Operazioni con i messaggi messi in quarantena (pagina 213).

8.3.1 Cartelle ricerche predefinite

Le cartelle di ricerche predefinite sono cartelle preconfigurate di ricerca che consentono l'accesso ai messaggi inseriti in quarantena in un periodo di tempo specifico o in base a un tipo particolare di posta inserita in quarantena. Per utilizzare le cartelle ricerche predefinite:

1. Selezionare il nodo **Quarantena**.



Schermata 113: cartelle ricerche predefinite

2. Per accedere alla cartella di ricerca, selezionarla dall'area **Cartelle ricerche predefinite** o da un nodo di **Quarantena** . GFI MailEssentials cercherà e visualizzerà in automatico tutti i messaggi inseriti in quarantena che rispondono ai criteri di ricerca della cartella di ricerca predefinita.

Le cartelle ricerche predefinite disponibili sono:

- **Basate su tempo:**
  - Oggi
  - Ieri
  - Settimana corrente
- **Basate su categoria:**
  - Tutti gli elementi malware e contenuti
  - Tutti gli elementi spam

> **NOTA**
> Utilizza i risultati di ricerca per rivedere le e-mail in quarantena. È possibile approvare i falsi positivi per recapitarli ai destinatari. Per ulteriori informazioni, fare riferimento a Operazioni con i messaggi messi in quarantena (pagina 213).

8.3.2 Creazione, modifica e rimozione delle cartelle ricerche predefinite dalle ricerche

1. Selezionare il nodo **Quarantena**.

2. Creare una nuova ricerca per i messaggi inseriti in quarantena. Per ulteriori informazioni, fare riferimento a Ricerca nella quarantena (pagina 203).

3. Nella pagina dei risultati, fare clic su **Salva come cartella di ricerca** e digitare un nome facilmente identificabile per la nuova cartella di ricerca.

La cartella di ricerca appena creata verrà elencata nel nodo **Quarantena > Cartelle ricerche**.

> **NOTA**
> Per modificare o eliminare una cartella di ricerca creata in precedenza, accedere alla cartella di ricerca e fare clic su **Modifica cartella di ricerca** o **Elimina cartella di ricerca**.

8.3.3 Utilizzo del nodo Cartelle ricerche per eliminare in automatico i messaggi inseriti in quarantena

Il nodo **Cartelle ricerche** consente di creare cartelle ricerche e impostare un valore di eliminazione automatica (in giorni). Quando un messaggio inserito in quarantena supera il numero indicato di giorni nella quarantena, il messaggio viene eliminato.

1. Selezionare **Quarantena > nodo Cartelle ricerche**.

2. Configurare una nuova cartella di ricerca per i messaggi da eliminare regolarmente sulla base delle istruzioni nel presente capitolo.

3. Selezionare **Abilita eliminazione automatica** e indicare il numero di giorni per cui conservare i messaggi.

4. Fare clic su **Salva cartella**.

8.4 Operazioni con i messaggi messi in quarantena

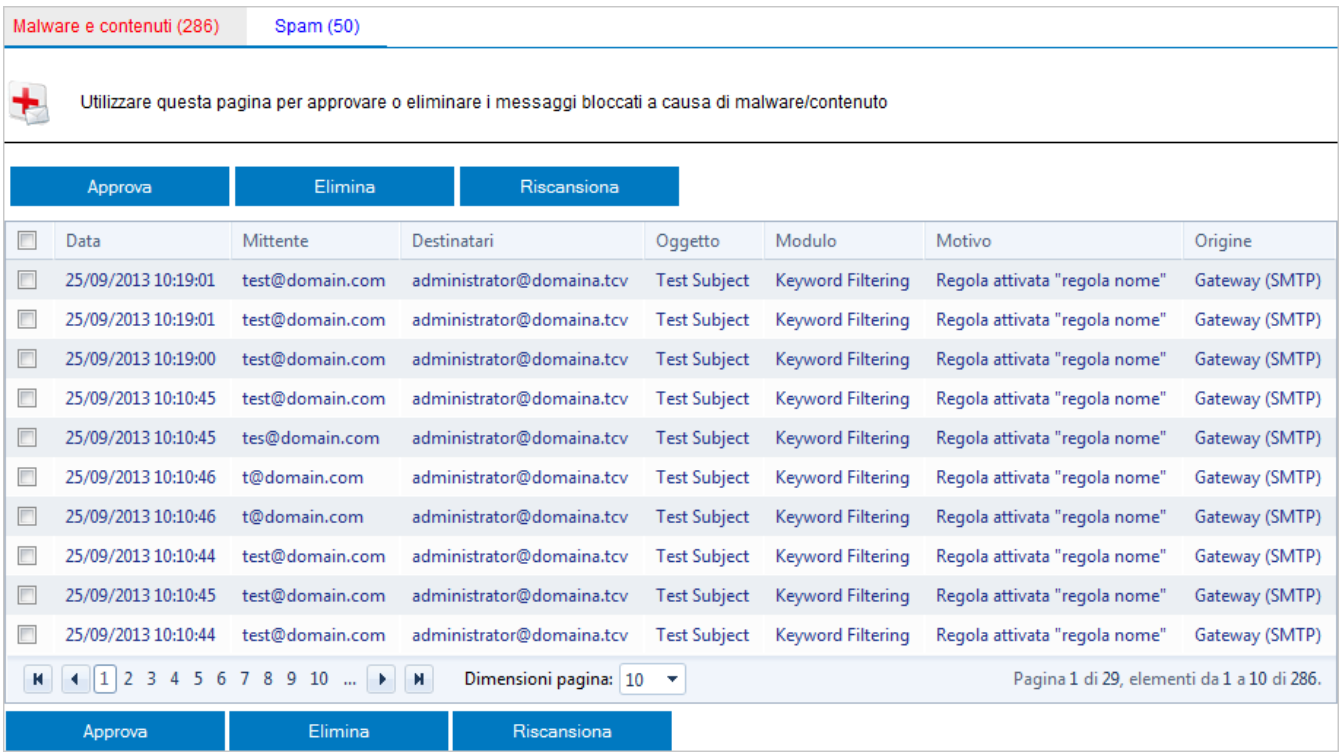
All'interno di GFI MailEssentials vi è una serie di azioni che è possibile eseguire sui messaggi inseriti in quarantena.

Quarantine Store è accessibile dall'interfaccia di GFI MailEssentials e l'amministratore può gestire i messaggi inseriti in quarantena.

Per accedere a GFI MailEssentials Quarantine Store, selezionare **GFI MailEssentials > Quarantena**.

8.4.1 Visualizzazione dei messaggi di posta elettronica inseriti in quarantena

La ricerca all'interno della quarantena o utilizzando le cartelle di ricerca predefinite o personalizzate riporta un elenco di messaggi inseriti in quarantena.


Malware e contenuti (286)
Spam (50)
Utilizzare questa pagina per approvare o eliminare i messaggi bloccati a causa di malware/contenuto
Approva
Elimina
Riscansiona
Data
Mittente
Destinatari
Oggetto
Modulo
Motivo
Origine
25/09/2013 10:19:01 test@domain.com administrator@domaina.tcv Test Subject Keyword Filtering Regola attivata "regola nome" Gateway (SMTP)
25/09/2013 10:19:01 test@domain.com administrator@domaina.tcv Test Subject Keyword Filtering Regola attivata "regola nome" Gateway (SMTP)
25/09/2013 10:19:00 test@domain.com administrator@domaina.tcv Test Subject Keyword Filtering Regola attivata "regola nome" Gateway (SMTP)
25/09/2013 10:10:45 test@domain.com administrator@domaina.tcv Test Subject Keyword Filtering Regola attivata "regola nome" Gateway (SMTP)
25/09/2013 10:10:45 tes@domain.com administrator@domaina.tcv Test Subject Keyword Filtering Regola attivata "regola nome" Gateway (SMTP)
25/09/2013 10:10:46 t@domain.com administrator@domaina.tcv Test Subject Keyword Filtering Regola attivata "regola nome" Gateway (SMTP)
25/09/2013 10:10:46 t@domain.com administrator@domaina.tcv Test Subject Keyword Filtering Regola attivata "regola nome" Gateway (SMTP)
25/09/2013 10:10:44 test@domain.com administrator@domaina.tcv Test Subject Keyword Filtering Regola attivata "regola nome" Gateway (SMTP)
25/09/2013 10:10:45 test@domain.com administrator@domaina.tcv Test Subject Keyword Filtering Regola attivata "regola nome" Gateway (SMTP)
25/09/2013 10:10:44 test@domain.com administrator@domaina.tcv Test Subject Keyword Filtering Regola attivata "regola nome" Gateway (SMTP)
1 2 3 4 5 6 7 8 9 10 ...
Dimensioni pagina: 10
Pagina 1 di 29, elementi da 1 a 10 di 286.
Approva
Elimina
Riscansiona

Schermata 114: Cerca risultati

NOTA

La pagina dei risultati può essere suddivisa in due schede:

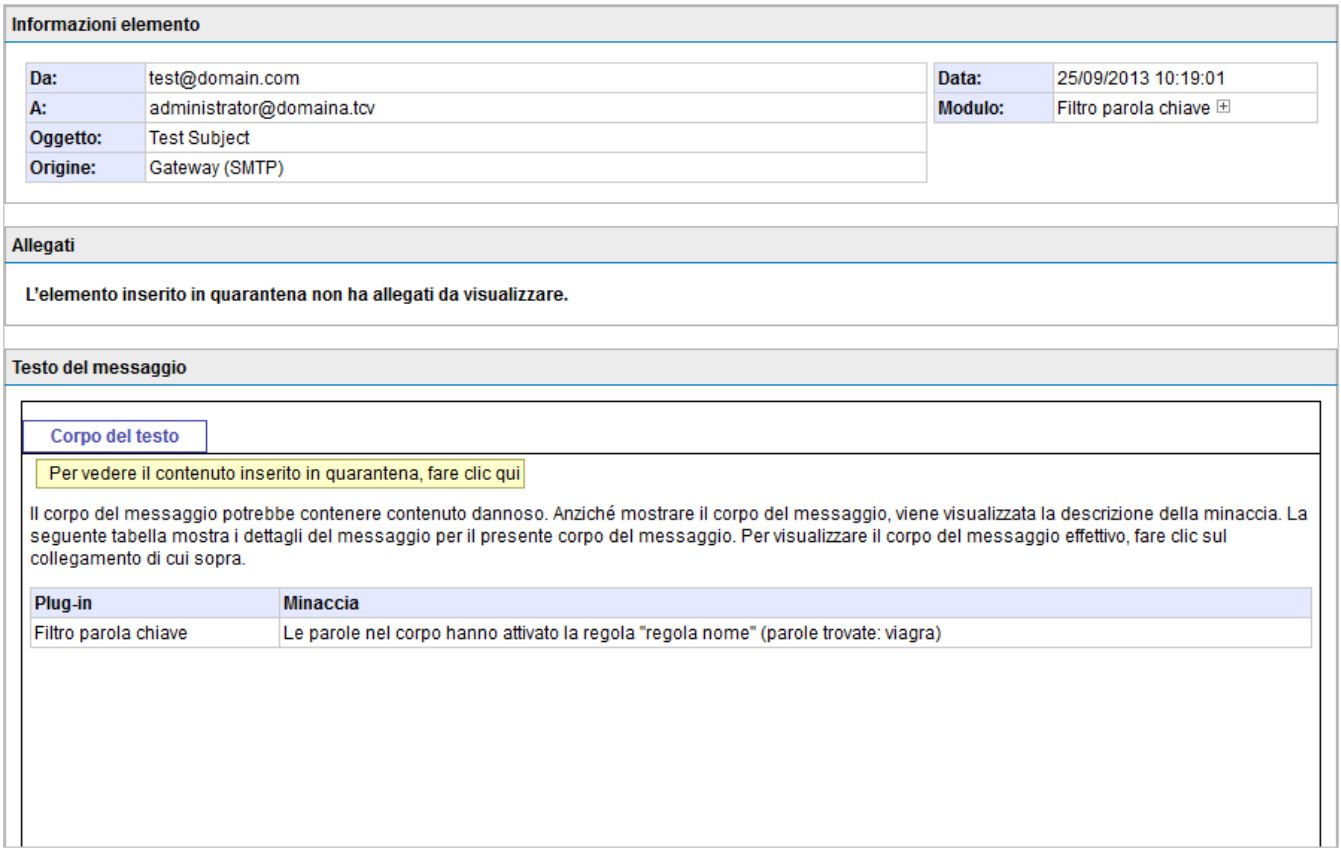
» **Malware e contenuti**: i messaggi bloccati dai motori antimalware e dalle regole di filtro dei contenuti.

» **Spam**: messaggi bloccati dai filtri antispam.

1. Scegliere la scheda **Malware e contenuti** oppure **Spam** per visualizzare i messaggi inseriti in quarantena di un tipo di messaggio specifico. La pagina dei risultati offre le seguenti funzioni e dettagli:

Opzione	Descrizione
Indietro	Riporta l'utente alla schermata precedente.
Approva	Consente di approvare un messaggio singolo o più d'uno. Per ulteriori informazioni, fare riferimento a Approvazione messaggi inseriti in quarantena (pagina 215).
Elimina	Elimina un messaggio singolo o più d'uno. Per ulteriori informazioni, fare riferimento a Eliminazione definitiva dei messaggi inseriti in quarantena (pagina 216).
Riscansiona	Riscansiona i messaggi utilizzando le firme antivirus attuali, che potrebbero essere più aggiornate delle firme antivirus inserite in quarantena nel messaggio. Selezionare uno o più messaggi, quindi fare clic su **Riscansiona** per eseguire nuovamente la scansione.
Modulo	Il modulo che ha identificato il messaggio da inserire in quarantena.
Motivo	Il motivo/regola che ha attivato l'azione per l'inserimento del messaggio in quarantena.
Mittente	L'indirizzo di posta elettronica del mittente.
Destinatari	L'indirizzo di posta elettronica del destinatario.
Oggetto	L'oggetto del messaggio inviato dal mittente.
Data	La data in cui il messaggio è stato inserito in quarantena.
Origine	Il percorso da cui è stato inserito in quarantena il messaggio.
Origine elemento	Consente di scegliere un'origine per il filtraggio della visualizzazione. Le opzioni disponibili sono: » Visualizza tutto » Archivio informazioni (VSAPI) » Gateway (SMTP) » Archivio informazioni (trasporto)
Dimensioni pagina	Consente la personalizzazione del numero di messaggi per pagina attualmente visualizzati. Scegliere un numero per visualizzare il numero massimo di elementi per pagina.

2. Per accedere ai dettagli del messaggio singolo, fare clic su una riga.


Informazioni elemento
Da: test@domain.com
A: administrator@domaina.tcv
Oggetto: Test Subject
Origine: Gateway (SMTP)
Data: 25/09/2013 10:19:01
Modulo: Filtro parola chiave
Allegati
L'elemento inserito in quarantena non ha allegati da visualizzare.
Testo del messaggio
Corpo del testo
Per vedere il contenuto inserito in quarantena, fare clic qui
Il corpo del messaggio potrebbe contenere contenuto dannoso. Anziché mostrare il corpo del messaggio, viene visualizzata la descrizione della minaccia. La seguente tabella mostra i dettagli del messaggio per il presente corpo del messaggio. Per visualizzare il corpo del messaggio effettivo, fare clic sul collegamento di cui sopra.
Plug-in
Minaccia
Filtro parola chiave
Le parole nel corpo hanno attivato la regola "regola nome" (parole trovate: viagra)

Schermata 115: dettagli elementi messi in quarantena

dalla pagina **Dettagli elementi messi in quarantena**, rivedere i dettagli del messaggio ed effettuare le seguenti operazioni.

Azione	Descrizione
Approva	Approvare il messaggio. Per ulteriori informazioni, fare riferimento a Approvazione messaggi inseriti in quarantena (pagina 215).
Disinfetta e approva	Disinfettare e approvare il messaggio. Per ulteriori informazioni, fare riferimento a Approvazione messaggi inseriti in quarantena (pagina 215).
Riscansiona	Riscansiona i messaggi utilizzando le firme antivirus attuali, che potrebbero essere più aggiornate delle firme antivirus inserite in quarantena nel messaggio.
Elimina	Eliminare il messaggio. Per ulteriori informazioni, fare riferimento a Eliminazione definitiva dei messaggi inseriti in quarantena (pagina 216).
Elimina e notifica	Eliminare il messaggio e notificare l'utente. Per ulteriori informazioni, fare riferimento a Eliminazione definitiva dei messaggi inseriti in quarantena (pagina 216).
Scarica elemento	Scarica il messaggio inserito in quarantena in un percorso a piacere utilizzando il formato .eml. **Avviso:** **I messaggi in Quarantine Store potrebbero presentare contenuto dannoso. utilizzare questa caratteristica con attenzione.**

8.4.2 Approvazione messaggi inseriti in quarantena

Potrebbero esserci delle istanze in cui voler approvare un messaggio bloccato da GFI MailEssentials. GFI MailEssentials consente all'amministratore di approvare un messaggio inserito in quarantena in modo da rilasciarlo da Quarantine Store e recapitarlo ai destinatari previsti.

Per approvare i messaggi:

1. Utilizzare le funzionalità di ricerca descritte nelle sezioni precedenti per restituire un elenco di messaggi inseriti in quarantena.

2. Selezionare la casella di controllo accanto ai messaggi inseriti in quarantena da approvare e fare clic su **Approva**.

Disinfezione e approvazione messaggi

GFI MailEssentials consente anche di rimuovere l'elemento che ha portato all'inserimento in quarantena del messaggio, per procedere poi con l'invio al destinatario.

Per disinfettare e approvare i messaggi:

1. Utilizzare le funzionalità di ricerca descritte nelle sezioni precedenti per restituire un elenco di messaggi inseriti in quarantena.

2. Fare clic su un messaggio per visualizzarne i dettagli.

3. Fare clic su **Disinfetta e approva**.

> **NOTA**
> I messaggi inseriti in quarantena dall'origine Information Store (VSAPI) non possono essere disinfettati.

8.4.3 Eliminazione definitiva dei messaggi inseriti in quarantena

1. Utilizzare le funzionalità di ricerca descritte nelle sezioni precedenti per restituire un elenco di messaggi inseriti in quarantena.

2. Selezionare la casella di controllo accanto ai messaggi inseriti in quarantena e fare clic su **Elimina**.

Eliminazione dei messaggi inseriti in quarantena e notifica all'utente

La funzione Elimina e notifica consente la notifica ai destinatari al momento di eliminare i messaggi dalla quarantena.

Per eliminare e notificare i destinatari:

1. Utilizzare le funzionalità di ricerca descritte nelle sezioni precedenti per restituire un elenco di messaggi inseriti in quarantena.

2. Fare clic su un messaggio per visualizzarne i dettagli.

3. Fare clic su **Elimina e notifica**.

8.5 Feed RSS quarantena

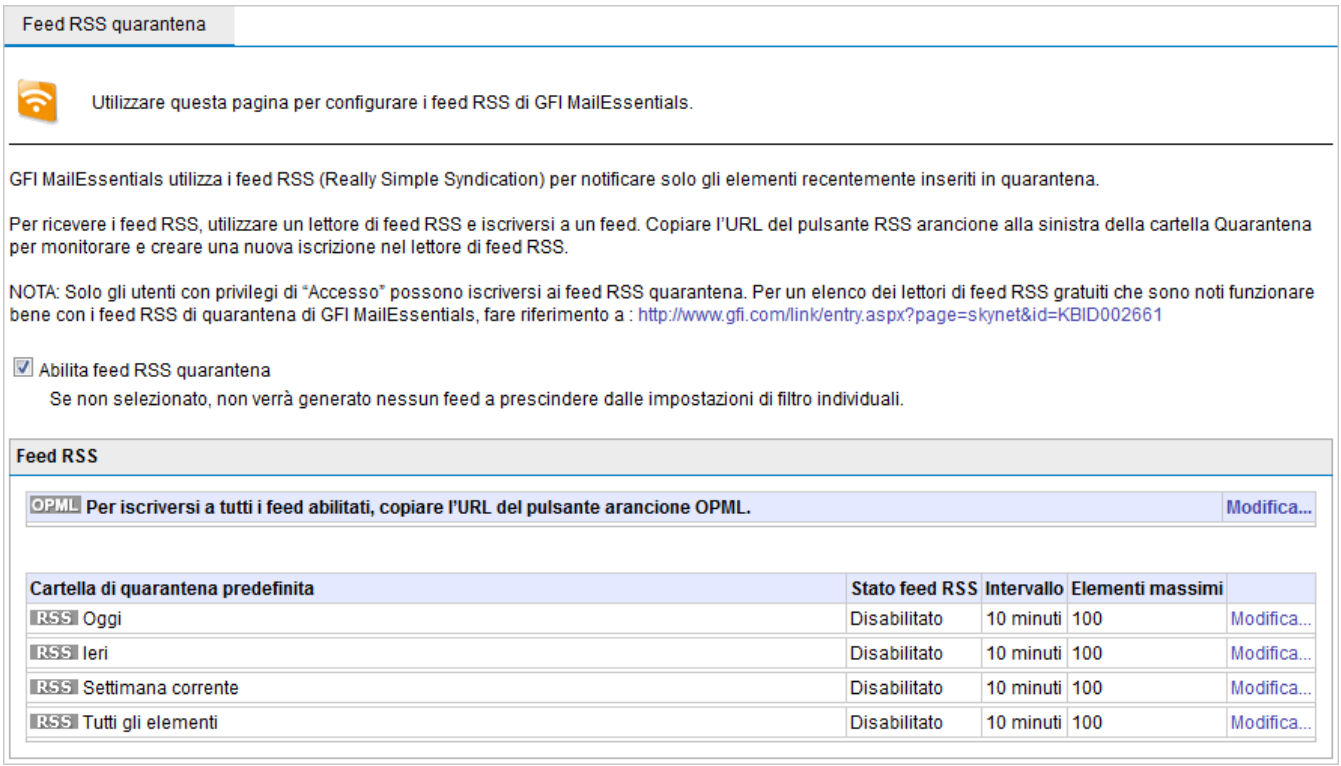
RSS (Really Simple Syndication) è un protocollo utilizzato per la distribuzione di contenuto o feed di aggiornamento, ad esempio le news, con i relativi iscritti. Per visualizzare i feed RSS, gli iscritti devono disporre di un lettore di feed apposito. Normalmente, i feed RSS includono un riepilogo del contenuto e un collegamento per visualizzare l'intero articolo.

Per facilitare il monitoraggio dei messaggi inseriti in quarantena è possibile utilizzare i feed RSS. Il feed di quarantena di GFI MailEssentials visualizza i messaggi inseriti in quarantena da rivedere, consentendo agli utenti di approvarli o eliminarli.

> **NOTA**
> I feed di quarantena RSS di GFI MailEssentials sono compatibili con la maggioranza dei lettori di feed RSS. Per un elenco dei lettori di feed RSS gratuiti che sono stati sperimentati con i feed RSS di quarantena di GFI MailEssentials, fare riferimento a:
> http://kbase.gfi.com/showarticle.asp?id=KBID002661

8.5.1 Abilitazione feed RSS quarantena

1. Selezionare **GFI MailEssentials > Quarantena > Feed RSS quarantena**.


Feed RSS quarantena
Utilizzare questa pagina per configurare i feed RSS di GFI MailEssentials.
GFI MailEssentials utilizza i feed RSS (Really Simple Syndication) per notificare solo gli elementi recentemente inseriti in quarantena.
Per ricevere i feed RSS, utilizzare un lettore di feed RSS e iscriversi a un feed. Copiare l'URL del pulsante RSS arancione alla sinistra della cartella Quarantena per monitorare e creare una nuova iscrizione nel lettore di feed RSS.
NOTA: Solo gli utenti con privilegi di "Accesso" possono iscriversi ai feed RSS quarantena. Per un elenco dei lettori di feed RSS gratuiti che sono noti funzionare bene con i feed RSS di quarantena di GFI MailEssentials, fare riferimento a : http://www.gfi.com/link/entry.aspx?page=skynet&id=KBID002661
Abilita feed RSS quarantena
Se non selezionato, non verrà generato nessun feed a prescindere dalle impostazioni di filtro individuali.
Feed RSS
OPML Per iscriversi a tutti i feed abilitati, copiare l'URL del pulsante arancione OPML.
Modifica...
Cartella di quarantena predefinita
Stato feed RSS
Intervallo
Elementi massimi
RSS Oggi
Disabilitato
10 minuti
100
Modifica...
RSS Ieri
Disabilitato
10 minuti
100
Modifica...
RSS Settimana corrente
Disabilitato
10 minuti
100
Modifica...
RSS Tutti gli elementi
Disabilitato
10 minuti
100
Modifica...

Schermata 116: feed RSS quarantena

2. Selezionare la casella di controllo **Abilita feed RSS quarantena**.

3. Dall'area **Feed RSS**, fare clic su **Modifica** nel lato destro della cartella di ricerca di quarantena per cui abilitare i feed RSS.

4. Selezionare la casella di controllo **Abilita feed quarantina RSS in questa cartella**.

5. Nella casella di testo **Aggiorna contenuto feed ogni**, indicare l'intervallo di aggiornamento in minuti. Il valore predefinito è 10 minuti.

6. Nella casella di testo **Il feed deve contenere al massimo**, indicare il numero massimo di elementi da includere nel feed. Il valore predefinito è 100 elementi.

> **NOTA**
> L'URL di un feed RSS può essere modificato facendo clic su **Reimposta URL feed**. Per modificare l'URL di tutti i feed RSS abilitati, fare clic su **Modifica** alla destra della voce **OPML**, quindi fare clic su **Reimposta tutti gli URL**. Quando si modifica l'URL, assicurarsi di aggiornare di conseguenza tutte le iscrizioni attuali.
> La reimpostazione dell'url del feed dovrebbe essere eseguita in caso di accesso non autorizzato.

7. Fare clic su **Applica**.

8.5.2 Iscrizione ai feed RSS quarantena

Iscrizione a tutti i feed RSS di quarantena abilitati

1. Selezionare **GFI MailEssentials > Quarantena > Feed RSS quarantena**.

2. Nell'area Feed RSS, fare clic con il pulsante destro del mouse sull'icona OPML, quindi selezionare **Copia collegamento** per copiare l'URL del feed RSS.

3. Utilizzare l'URL copiato nell'applicazione del lettore di feed RSS così da creare una nuova iscrizione al feed RSS.

Iscrizione a un feed RSS di quarantena della cartella di ricerca

Per iscriversi al feed RSS di una cartella di ricerca predefinita o personalizzata:

1. Selezionare **GFI MailEssentials > Quarantena > Feed RSS quarantena**.

2. Nell'area Feed RSS, fare clic con il pulsante destro del mouse sull'icona RSS accanto alla cartella di ricerca a cui iscriversi, quindi selezionare **Copia collegamento** per copiare l'URL del feed RSS.

3. Utilizzare l'URL copiato nell'applicazione del lettore di feed RSS così da creare una nuova iscrizione al feed RSS.

8.5.3 Protezione accesso ai feed RSS di quarantena di GFI MailEssentials

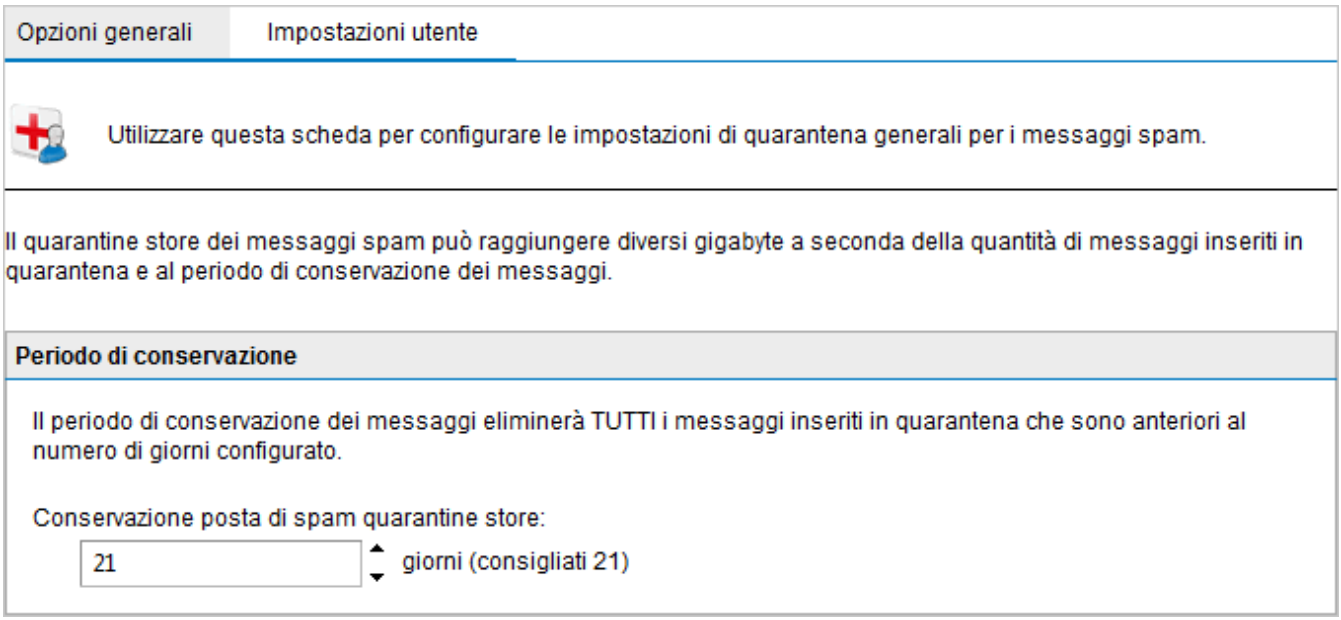
Dal nodo Controllo di accesso di GFI MailEssentials Configuration è possibile configurare gli utenti che possono iscriversi ai feed di quarantena RSS. Per ulteriori informazioni, fare riferimento a Controllo di accesso (pagina 248).

8.6 Opzioni quarantena

Utilizzare Opzioni quarantena per configurare la conservazione dello spam in quarantena, la creazione di report per l'utente e la configurazione utente inesistente malware in quarantena.

8.6.1 Opzioni spam

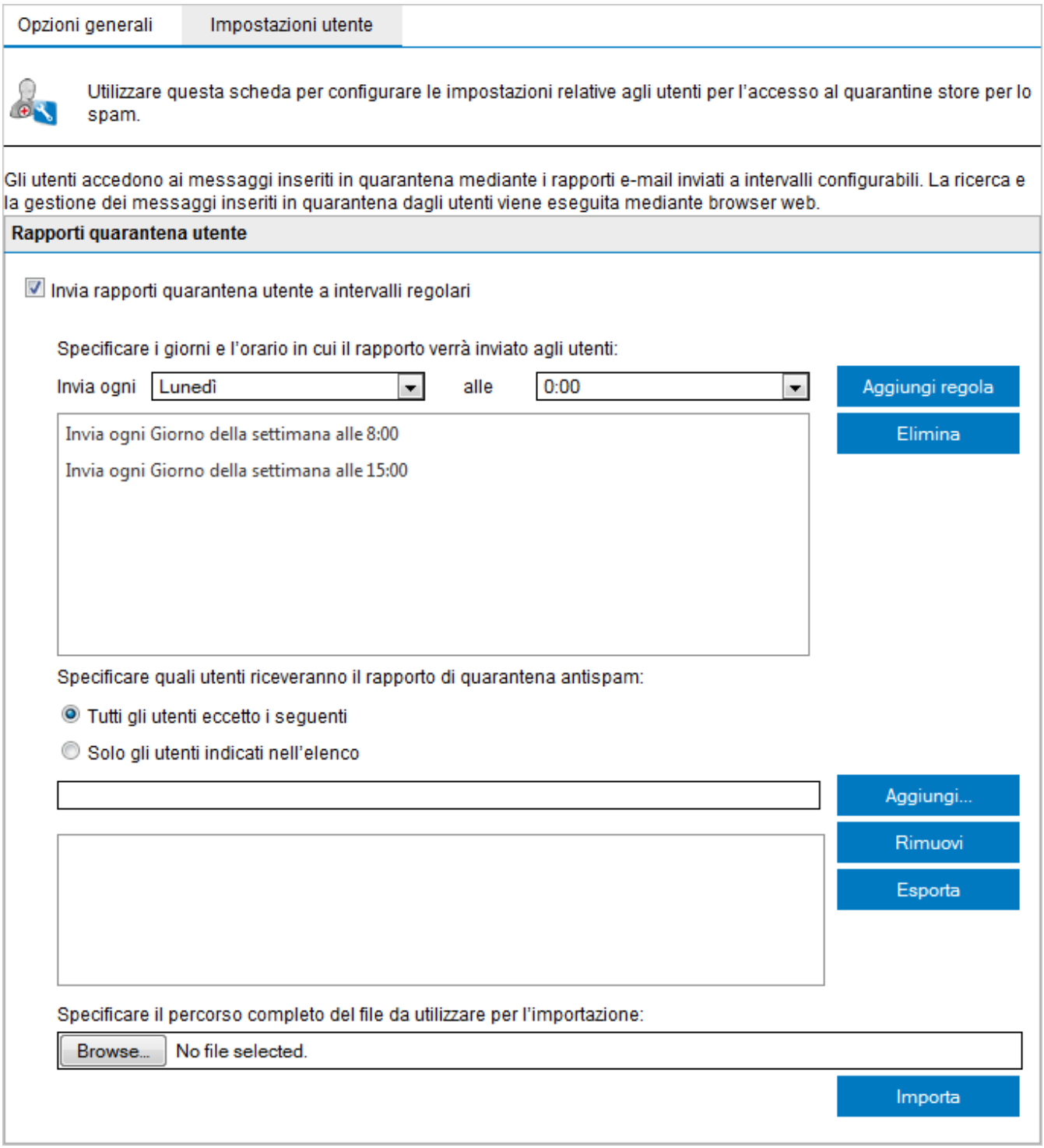
1. Selezionare **Quarantena > Opzioni quarantena > Opzioni spam**.


Opzioni generali
Impostazioni utente
Utilizzare questa scheda per configurare le impostazioni di quarantena generali per i messaggi spam.
Il quarantine store dei messaggi spam può raggiungere diversi gigabyte a seconda della quantità di messaggi inseriti in quarantena e al periodo di conservazione dei messaggi.
Periodo di conservazione
Il periodo di conservazione dei messaggi eliminerà TUTTI i messaggi inseriti in quarantena che sono anteriori al numero di giorni configurato.
Conservazione posta di spam quarantine store:
21
giorni (consigliati 21)

Schermata 117: opzioni spam - scheda Opzioni generali

2. Dalla scheda **Opzioni generali**, modificare o mantenere il periodo di **Conservazione posta di spam quarantine store.**

3. Fare clic sulla scheda **Impostazioni utente.**


Opzioni generali
Impostazioni utente
Utilizzare questa scheda per configurare le impostazioni relative agli utenti per l'accesso al quarantine store per lo spam.
Gli utenti accedono ai messaggi inseriti in quarantena mediante i rapporti e-mail inviati a intervalli configurabili. La ricerca e la gestione dei messaggi inseriti in quarantena dagli utenti viene eseguita mediante browser web.
Rapporti quarantena utente
Invia rapporti quarantena utente a intervalli regolari
Specificare i giorni e l'orario in cui il rapporto verrà inviato agli utenti:
Invia ogni
Lunedì
alle
0:00
Aggiungi regola
Elimina
Invia ogni Giorno della settimana alle 8:00
Invia ogni Giorno della settimana alle 15:00
Specificare quali utenti riceveranno il rapporto di quarantena antispam:
Tutti gli utenti eccetto i seguenti
Solo gli utenti indicati nell'elenco
Aggiungi...
Rimuovi
Esporta
Specificare il percorso completo del file da utilizzare per l'importazione:
Browse...
No file selected.
Importa

Schermata 118: opzioni spam - scheda Impostazioni utente

4. Selezionare **Invia rapporti quarantena utente a intervalli regolari** per abilitare l'invio di rapporti di quarantena agli utenti.

NOTA

I rapporti quarantena utente sono messaggi regolari inviati agli utenti e contenenti un elenco di spam bloccato per quell'utente specifico. Utilizzando questo elenco, gli utenti possono controllare e approvare eventuali messaggi attendibili. I messaggi bloccati dai filtri Malware e contenuti non sono visualizzati in questi messaggi.

5. Configurare la frequenza di invio del rapporto. Per aggiungerla alla pianificazione preimpostata, selezionare una data e un orario, quindi fare clic su **Aggiungi regola.** Selezionare una data e ora esistenti, quindi fare clic su **Elimina** per eliminare la data/ora selezionate.

6. Configurare gli utenti che riceveranno i rapporti di spam in quarantena. Selezionare **Tutti gli utenti eccetto i seguenti** o **Solo gli utenti indicati nell'elenco**, quindi fornire l'indirizzo di posta degli utenti da includere o escludere.

NOTA

Fare clic su **Sfoglia** per selezionare un file con l'elenco di indirizzi di posta da importare, quindi fare clic su **Importa**.

7. Fare clic su **Applica**.

8.6.2 Opzioni malware

GFI MailEssentials può anche essere configurato per notificare tramite messaggio (Modulo azione quarantena) all'amministratore o agli utenti autorizzati ogni volta che un messaggio viene inserito in quarantena.

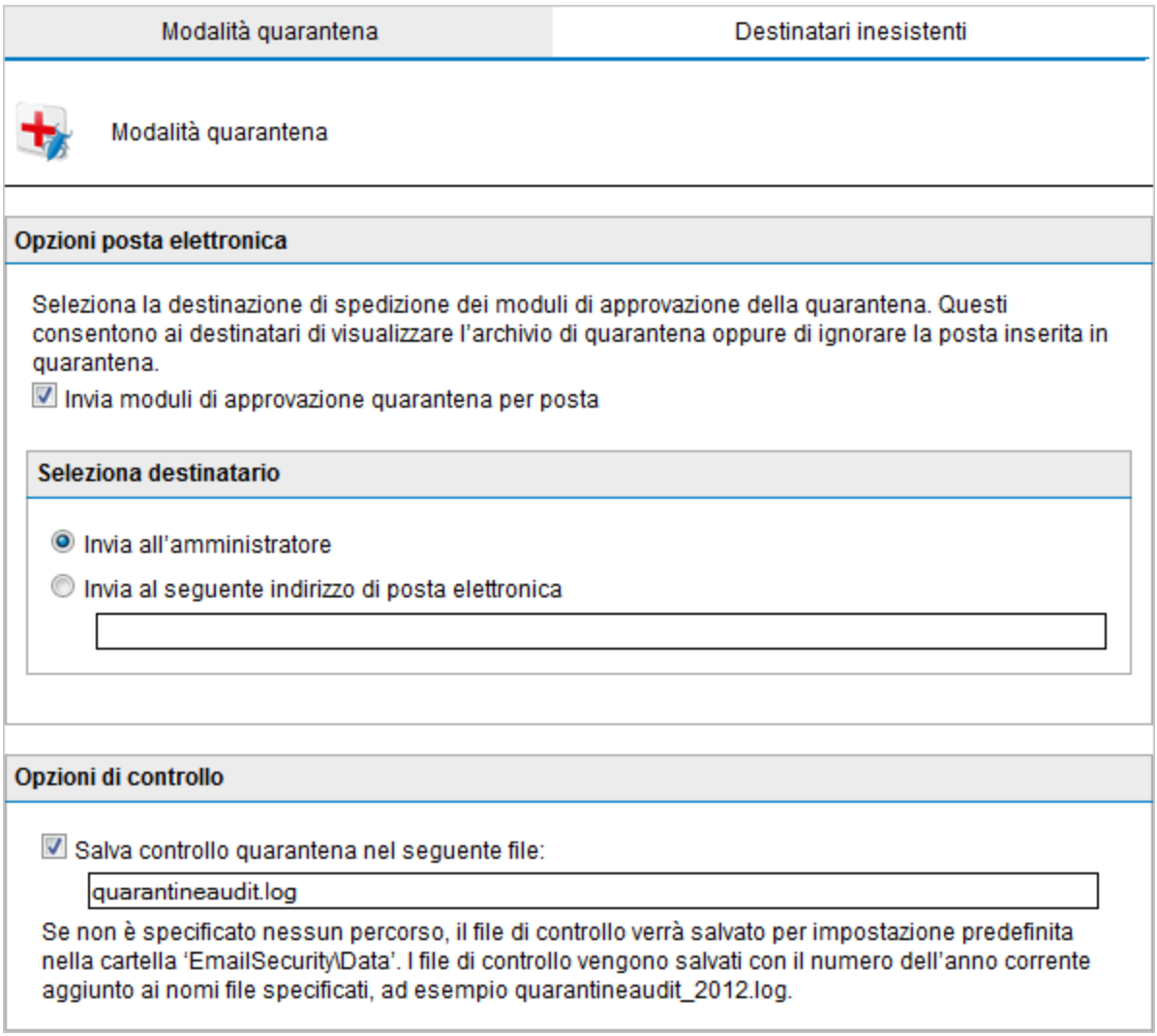
Il modulo di approvazione quarantena contiene dati relativi al messaggio inserito in quarantena, tra cui il motivo per cui è stato bloccato ed eventuali allegati inclusi nel messaggio. L'amministratore può quindi agire sul messaggio inserito in quarantena (ad esempio approvarlo) direttamente dal client di posta.

NOTA

Per eliminare automaticamente i messaggi più vecchi di un numero specifico di giorni, creare una nuova cartella di ricerca e impostare la funzione di Eliminazione automatica dei messaggi dopo un numero di giorni specifico. Per ulteriori informazioni, fare riferimento a Utilizzo del nodo Cartelle ricerche per eliminare in automatico i messaggi inseriti in quarantena (pagina 212).

Abilitazione moduli di approvazione quarantena

1. Selezionare **Quarantena > Opzioni quarantena > Opzioni malware**.


Modalità quarantena
Destinatari inesistenti
Modalità quarantena
Opzioni posta elettronica
Seleziona la destinazione di spedizione dei moduli di approvazione della quarantena. Questi consentono ai destinatari di visualizzare l'archivio di quarantena oppure di ignorare la posta inserita in quarantena.
Invia moduli di approvazione quarantena per posta
Seleziona destinatario
Invia all'amministratore
Invia al seguente indirizzo di posta elettronica
Opzioni di controllo
Salva controllo quarantena nel seguente file:
quarantineaudit.log
Se non è specificato nessun percorso, il file di controllo verrà salvato per impostazione predefinita nella cartella 'EmailSecurity\Data'. I file di controllo vengono salvati con il numero dell'anno corrente aggiunto ai nomi file specificati, ad esempio quarantineaudit_2012.log.

Schermata 119: Modalità quarantena

2. Dalla scheda **Modalità quarantena**, selezionare la casella di controllo **Invia moduli di approvazione quarantena per posta** per abilitare l'invio dei moduli di approvazione quarantena.

3. Dall'area **Seleziona destinatario**, indicare il destinatario dei moduli di approvazione della quarantena:

Opzione	Descrizione
Invia all'amministratore	Invia i moduli di approvazione quarantena all'amministratore come configurato nel nodo **Impostazioni generali**. Per ulteriori informazioni, fare riferimento a Indirizzo e-mail amministratore (pagina 241).
Invia al seguente indirizzo di posta elettronica	Invia moduli di approvazione quarantena a un altro indirizzo di posta elettronica. Digitare il destinatario nella casella di testo fornita.

4. Facoltativo: selezionare **Salva controllo quarantena nel seguente file:** e configurare un nome file per salvare una copia del registro di quarantena.

5. Fare clic su **Applica**.

Destinatari inesistenti

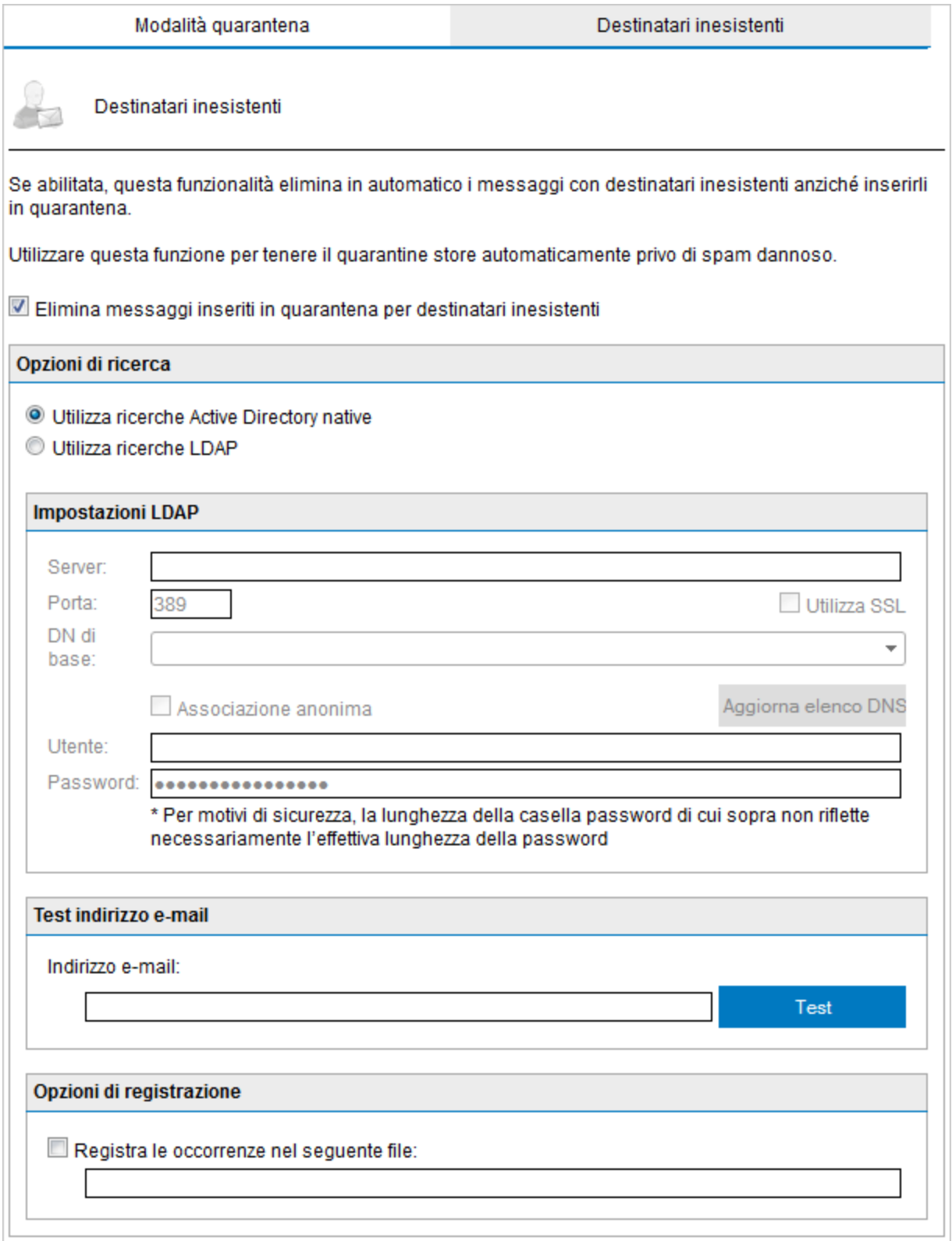
La funzione Destinatari inesistenti di GFI MailEssentials scansiona i messaggi alla ricerca di indirizzi di

posta locali inesistenti prima che siano memorizzati in Quarantine Store. Se un messaggio contiene indirizzi di posta locali inesistenti, verrà eliminato in modo permanente. In questo modo, si riduce il numero di messaggi di posta elettronica da sottoporre alla revisione amministrativa.

Configurazione destinatari inesistenti

Il filtro Destinatari inesistenti richiede l'accesso a un elenco di indirizzi locali. Questa operazione viene eseguita da Active Directory oppure, se la comunicazione con Active Directory non è possibile, tramite un server LDAP.

1. Selezionare **Quarantena > Opzioni quarantena > Opzioni malware**.


Modalità quarantena
Destinatari inesistenti
Destinatari inesistenti
Se abilitata, questa funzionalità elimina in automatico i messaggi con destinatari inesistenti anziché inserirli in quarantena.
Utilizzare questa funzione per tenere il quarantine store automaticamente privo di spam dannoso.
Elimina messaggi inseriti in quarantena per destinatari inesistenti
Opzioni di ricerca
Utilizza ricerche Active Directory native
Utilizza ricerche LDAP
Impostazioni LDAP
Server:
Porta:
389
Utilizza SSL
DN di base:
Associazione anonima
Aggiorna elenco DNS
Utente:
Password:
* Per motivi di sicurezza, la lunghezza della casella password di cui sopra non riflette necessariamente l'effettiva lunghezza della password
Test indirizzo e-mail
Indirizzo e-mail:
Test
Opzioni di registrazione
Registra le occorrenze nel seguente file:

Schermata 120: Destinatari inesistenti

2. Dalla scheda **Destinatari inesistenti**, selezionare la casella di controllo **Elimina messaggi inseriti in quarantena per destinatari inesistenti**.

3. Selezionare il metodo di ricerche utenti da utilizzare:

Opzione	Descrizione
Utilizza ricerche Active Directory native	Selezionare questa opzione se GFI MailEssentials è installato in modalità Active Directory e ha accesso a tutti gli utenti di Active Directory. Andare al passaggio 8. **NOTA** Quando GFI MailEssentials è installato in una modalità utente Active Directory in una DMZ, l'AD di una DMZ di solito non include tutti gli utenti di rete (destinatari della posta). In questo caso, configurare GFI MailEssentials per l'utilizzo delle ricerche LDAP. **NOTA** Quando GFI MailEssentials si trova dietro un firewall, questa funzione potrebbe non essere in grado di connettersi direttamente alla Active Directory interna a causa delle impostazioni del firewall. Utilizzare le ricerche LDAP per eseguire la connessione all'Active Directory interna della rete e assicurarsi di abilitare la porta predefinita 389 sul firewall.
Utilizza ricerche LDAP	Selezionare questa opzione quando GFI MailEssentials è installato in modalità SMTP e/o quando GFI MailEssentials non dispone di accesso diretto all'elenco completo degli utenti.

4. Specificare il nome del server LDAP o l'indirizzo IP nella casella di testo **Server**.

> **NOTA**
> In un ambiente Active Directory, normalmente il server LDAP è controller di dominio o catalogo globale.

5. Specificare il numero della porta nella casella di testo **Porta**. Il numero predefinito è 389. Se la connessione al server LDAP avviene tramite SSL, selezionare **Utilizza SSL**: la porta predefinita diventerà 636.

> **NOTA**
> Assicurarsi che la porta sia abilitata dal firewall.

6. Fare clic su **Aggiorna elenco DNS** per popolare l'elenco **DN di base** e scegliere il DN di base, quindi il livello superiore nella gerarchia di Active Directory.

7. Se il server LDAP richiede l'autenticazione, specificare **Utente** e **Password**. In alternativa, se non è richiesta l'autenticazione, selezionare **Associazione anonima**.

8. Verificare le impostazioni di configurazione indicando un indirizzo di posta valido nella casella **Indirizzo posta elettronica**, quindi fare clic su **Test**. Se l'indirizzo di posta elettronica non è presente, rivedere le impostazioni di configurazione.

9. Per registrare l'attività dei destinatari inesistenti in un file di registro, selezionare **Registra occorrenze nel seguente file**, quindi indicare il percorso e il nome del file (comprensivo di estensione .txt) di una posizione personalizzata su disco dove è possibile salvare il file di registro. In alternativa, indicare solo il nome del file (compresa l'estensione .txt) e il file di registro verrà salvato nel seguente percorso predefinito.

```
<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\\EmailSecurity\Logs\<nomefile>.txt
```

10. Fare clic su **Applica**.

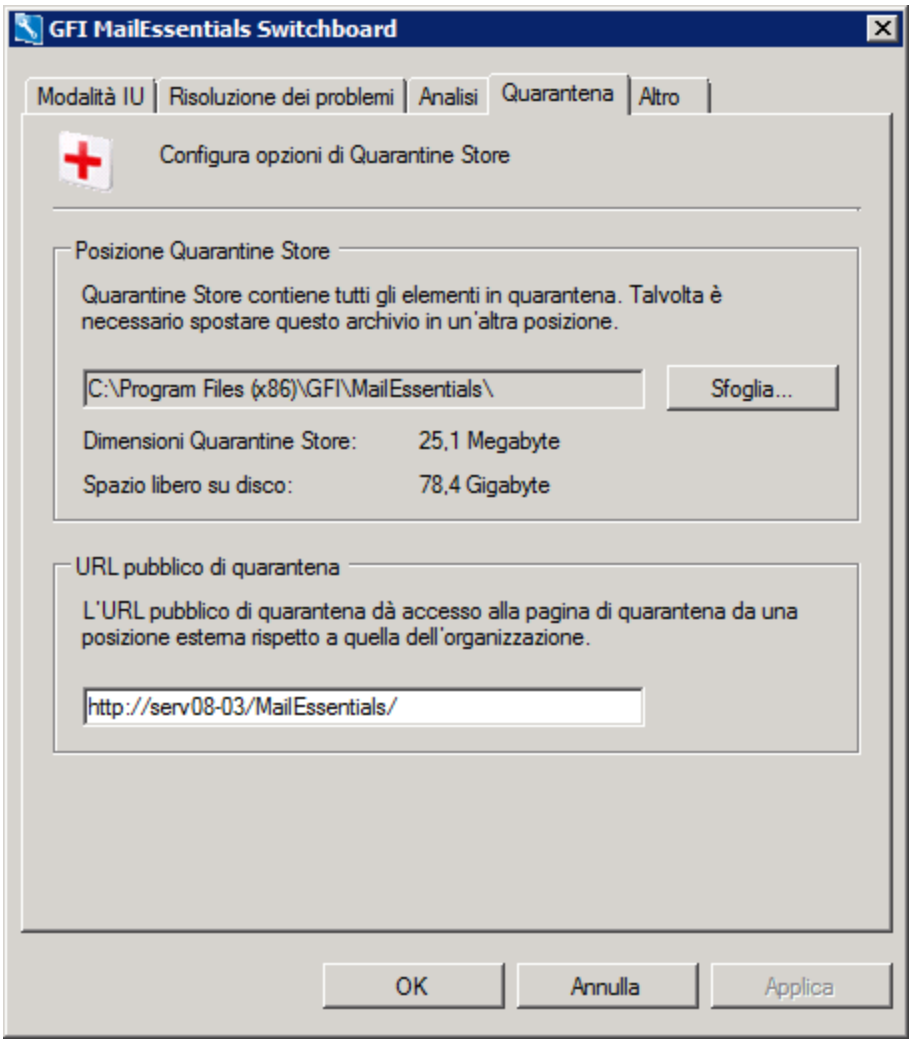
8.7 Percorso e URL pubblico di Quarantine Store

Utilizzare GFI MailEssentials Switchboard per configurare il percorso e l'URL pubblico di Quarantine Store.

Il percorso di Quarantine Store è la posizione in cui vengono salvati i messaggi inseriti in quarantena. Per impostazione predefinita, si trova nel percorso di installazione di GFI MailEssentials. Tuttavia, nei casi in cui lo spazio su disco sia insufficiente, potrebbe essere necessario lo spostamento in un percorso alternativo.

L'URL pubblico di quarantena dà accesso alla pagina di quarantena da una posizione esterna. Per impostazione predefinita, è basata sulle impostazioni della directory virtuale di IIS di GFI MailEssentials che sono state fornite durante l'installazione. Tuttavia, tale posizione potrebbe venire modificata se si inviano messaggi o notifiche digest della quarantena che vengono visualizzate al di fuori dalla rete interna. In tal caso, l'URL dovrà essere modificato in modo da essere raggiungibile via Internet.

1. Avviare GFI MailEssentials Switchboard da **Start > Tutti i programmi > GFI MailEssentials > Switchboard**.


GFI MailEssentials Switchboard
Modalità IU
Risoluzione dei problemi
Analisi
Quarantena
Altro
Configura opzioni di Quarantine Store
Posizione Quarantine Store
Quarantine Store contiene tutti gli elementi in quarantena. Talvolta è necessario spostare questo archivio in un'altra posizione.
C:\Program Files (x86)\GFI\MailEssentials\
Sfoglia...
Dimensioni Quarantine Store: 25,1 Megabyte
Spazio libero su disco: 78,4 Gigabyte
URL pubblico di quarantena
L'URL pubblico di quarantena dà accesso alla pagina di quarantena da una posizione esterna rispetto a quella dell'organizzazione.
http://serv08-03/MailEssentials/
OK
Annulla
Applica

Schermata 121: Percorso e URL pubblico di Quarantine Store

2. Dalla scheda **Quarantena**, fare clic su **Sfoglia** per selezionare un percorso alternativo per Quarantine Store.

IMPORTANTE

Assicurarsi che la partizione del disco dove viene salvato Quarantine Store disponga di spazio sufficiente. I messaggi spam non verranno messi in quarantena se lo spazio su disco è inferiore a 512 MB. Una volta raggiunti 512 MB, il funzionamento dell'e-mail in quarantena verrà arrestato e lo spam verrà etichettato e recapitato nelle cassette postali dei destinatari, finché lo spazio libero non sarà superiore a 512 MB.

3. Fornire un URL alternativo da utilizzare per l'accesso alla quarantena da un percorso esterno all'organizzazione.

4. Fare clic su **OK** per salvare la configurazione.

9 Gestione posta elettronica

GFI MailEssentials comprende un numero di strumenti che facilitano la gestione dei messaggi in entrata e in uscita.

Argomenti del presente capitolo:

9.1 Liberatorie **227**

9.2 Risposte automatiche **231**

9.3 Server elenco **233**

9.4 Monitoraggio posta elettronica **237**

9.1 Liberatorie

Le liberatorie sono contenuti standard aggiunti alla parte superiore o inferiore della posta in uscita per motivi legali e/o di marketing. Aiutano le aziende a proteggersi dalle minacce legali potenziali derivanti dai contenuti di un messaggio e ad aggiungere descrizioni per i prodotti/servizi offerti.

» Configurazione liberatorie

» Disabilitazione e abilitazione liberatorie

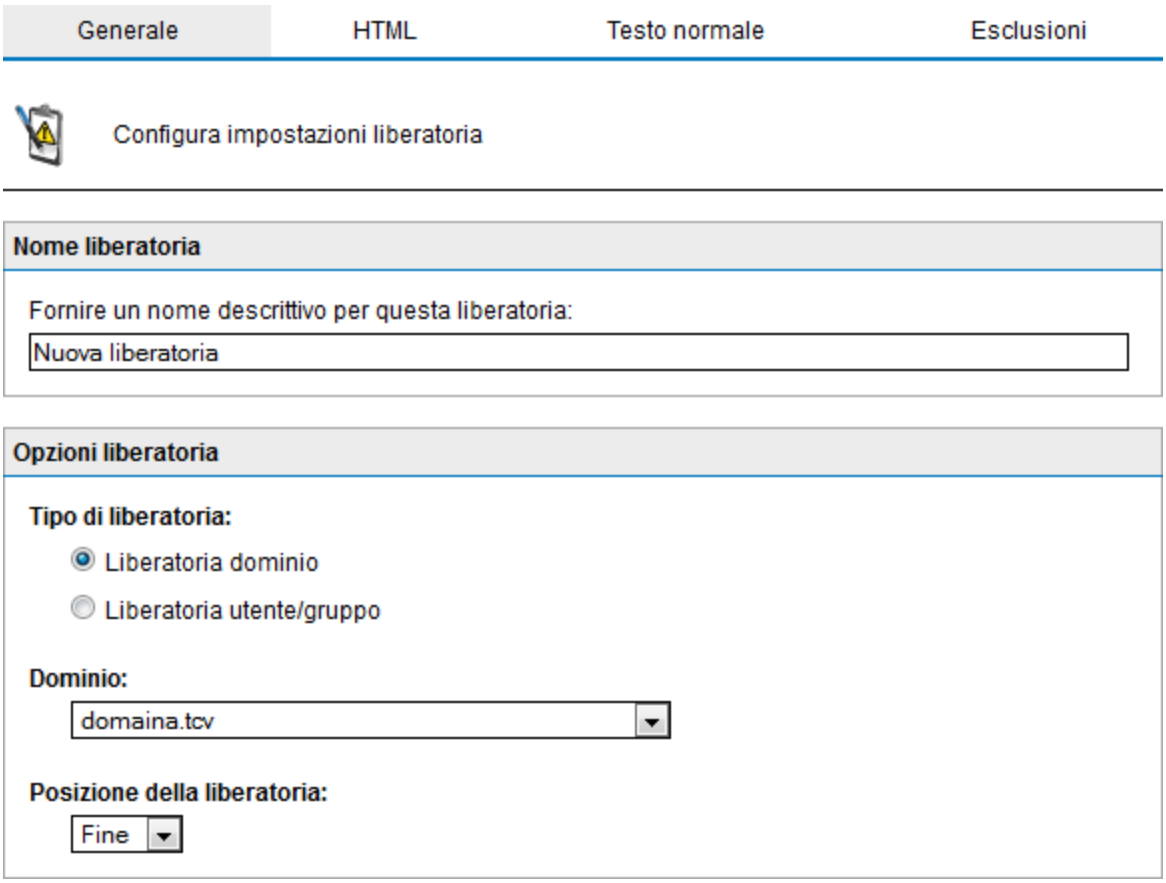
» Classificazione liberatorie per priorità

9.1.1 Configurazione liberatorie

Per personalizzare o creare una nuova liberatoria:

1. Selezionare **Gestione posta elettronica > Liberatorie**.

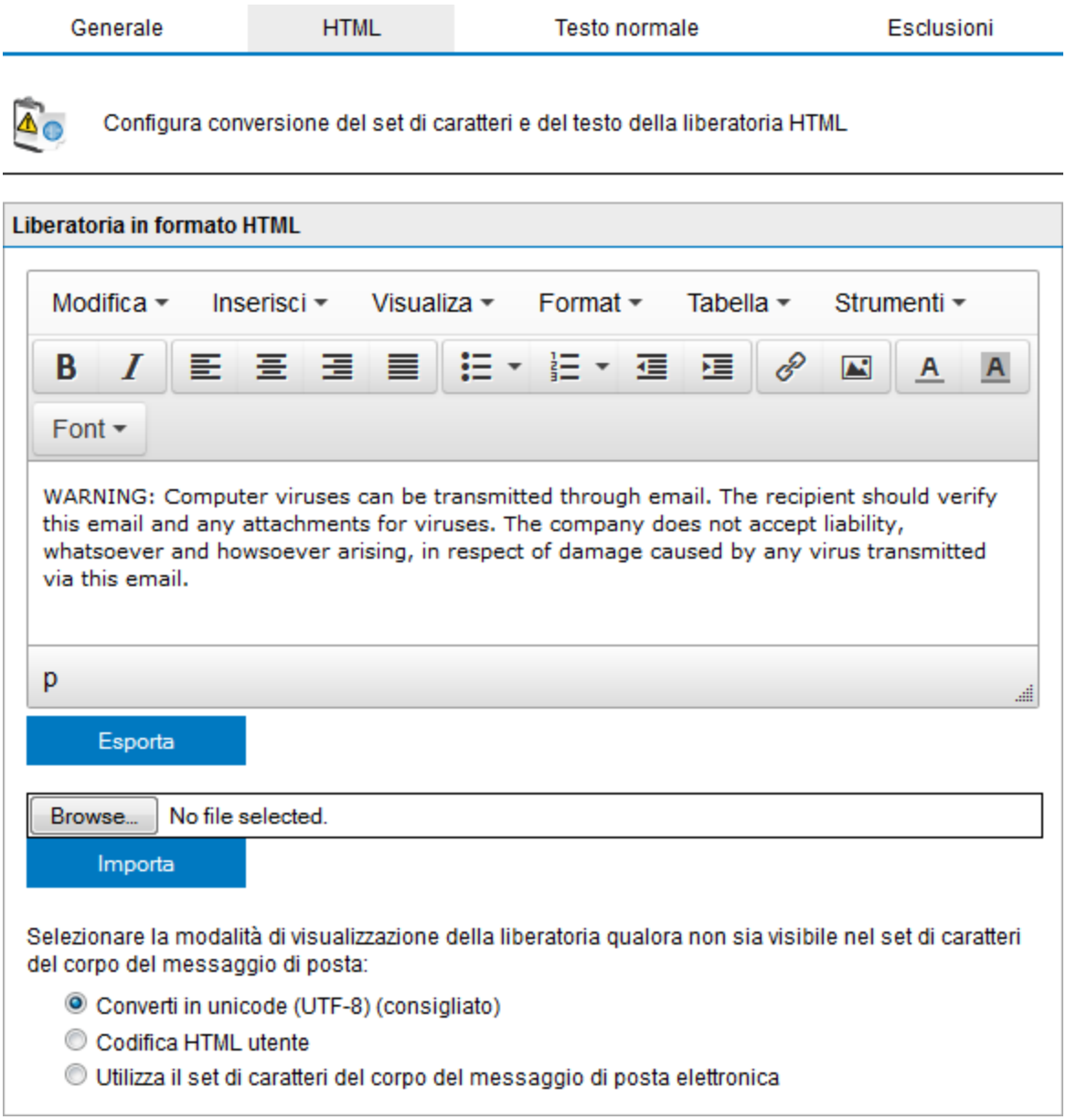
2. Fare clic su una liberatoria per modificarne le impostazioni o fare clic su **Aggiungi liberatoria** per crearne una nuova.



Schermata 122: aggiunta di una nuova liberatoria

3. Dalla scheda **Generale**, configurare quanto segue:

Opzione	Descrizione
Nome liberatoria	Digitare un nome univoco e descrittivo per la nuova liberatoria.
Tipo di liberatoria	Scegliere a quele utente applicare la liberatoria: » **Liberatoria dominio**: La liberatoria verrà aggiunta a tutti i messaggi inviati da un dominio. Selezionare il dominio dall'elenco a discesa **Dominio**. » **Liberatoria utente/gruppo**: Fare clic su **Cerca utente/gruppo** per selezionare un utente o gruppo di utenti a cui viene aggiunta la liberatoria per i messaggi in uscita. Se GFI MailEssentials è in modalità Active Directory, scegliere l'utente o i gruppi direttamente da Active Directory, altrimenti indicare l'indirizzo e-mail SMTP dell'utente.
Posizione della liberatoria	Selezionare l'opzione **Superiore** o **Fine** per scegliere se collocare la liberatoria nella parte superiore o inferiore del messaggio.


Generale
HTML
Testo normale
Esclusioni
Configura conversione del set di caratteri e del testo della liberatoria HTML
Liberatoria in formato HTML
Modifica
Inserisci
Visualizza
Format
Tabella
Strumenti
Font
WARNING: Computer viruses can be transmitted through email. The recipient should verify this email and any attachments for viruses. The company does not accept liability, whatsoever and howsoever arising, in respect of damage caused by any virus transmitted via this email.
p
Esporta
Browse...
No file selected.
Importa
Selezionare la modalità di visualizzazione della liberatoria qualora non sia visibile nel set di caratteri del corpo del messaggio di posta:
Converti in unicode (UTF-8) (consigliato)
Codifica HTML utente
Utilizza il set di caratteri del corpo del messaggio di posta elettronica

Schermata 123: Liberatoria in formato HTML

4. Dalla scheda **HTML**, utilizzare l'editor HTML per creare una liberatoria personalizzata in formato HTML. Per aggiungere campi all'e-mail o di Active Directory (variabili) alla liberatoria, selezionare **Inserisci > Variabile…**. Scegliere la variabile da aggiungere, quindi fare clic su **Aggiungi**.

> **NOTA**
> Le variabili del nome visualizzato e indirizzo e-mail del destinatario verranno incluse soltanto se il messaggio viene inviato a un singolo destinatario. Se i messaggi vengono inviati a più destinatari, le variabili saranno sostituite con i "destinatari".

5. Selezionare la codifica per la liberatoria HTML se il set di caratteri del corpo del messaggio non è impostato su HTML:

Opzione	Descrizione
Converti in unicode	Converte in Unicode sia il corpo del messaggio che le liberatorie, in modo da visualizzarli correttamente entrambi. (Consigliato)
Utilizza codifica HTML	Utilizzare questa opzione per definire i set di caratteri per il corpo del messaggio e la liberatoria.
Utilizza il set di caratteri del corpo del messaggio di posta elettronica	La liberatoria viene convertita nel set di caratteri del corpo del messaggio. **NOTA:** Se si sceglie questa opzione, una parte del testo potrebbe non venire visualizzata correttamente.

6. Selezionare la scheda **Testo normale** e immettere il testo da includere nei messaggi di testo normale direttamente nel campo **Liberatoria in formato testo**. In alternativa, aggiungere variabili alla liberatoria facendo clic su **Variabile…**. Le variabili che possono essere aggiunte sono: campi dell'e-mail (nome mittente, indirizzo e-mail destinatario, ecc...) o campi di Active Directory (nome, titolo, numeri di telefono, ecc...). Scegliere la variabile da aggiungere, quindi fare clic su **Aggiungi**.

> **NOTA**
> Le variabili del nome visualizzato e indirizzo e-mail del destinatario verranno incluse soltanto se il messaggio viene inviato a un singolo destinatario. Se i messaggi vengono inviati a più destinatari, le variabili saranno sostituite con i "destinatari".

7. Indicare la codifica da utilizzare per la liberatoria in testo normale se il set di caratteri del corpo del messaggio non è impostato su testo normale:

Opzione	Descrizione
Converti in unicode	Converte in Unicode sia il corpo del messaggio che le liberatorie, in modo da visualizzarli correttamente entrambi.
Utilizza il set di caratteri del corpo del messaggio di posta elettronica	La liberatoria viene convertita nel set di caratteri del corpo del messaggio. **NOTA:** Se si sceglie questa opzione, una parte del testo potrebbe non venire visualizzata correttamente.

8. Dalla scheda **Esclusioni**, indicare i mittenti o i destinatari a cui non applicare la liberatoria. Immettere l'indirizzo e-mail oppure fare clic su **Cerca** per cercare gli indirizzi e-mail in Active Directory. Fare clic su **Aggiungi** per aggiungere l'indirizzo e-mail all'elenco esclusione.

> **NOTA**
> Perché la liberatoria non sia inclusa nel messaggio, tutti i destinatari devono essere inclusi nell'elenco esclusioni.

9. Fare clic su **Applica** per salvare le impostazioni.

9.1.2 Disabilitazione e abilitazione liberatorie

Per impostazione predefinita, le liberatorie sono abilitate automaticamente. Per disabilitare o abilitare una liberatoria:

1. Selezionare **Gestione posta elettronica > Liberatorie**.

2. Selezionare le liberatorie da abilitare/disabilitare e fare clic su **Disabilita selezionati** o su **Abilita selezionati** per eseguire l'azione desiderata.

9.1.3 Classificazione liberatorie per priorità

È possibile personalizzare l'ordine di applicazione delle liberatorie ai messaggi in uscita. Se allo stesso utente sono abilitate e applicate più liberatorie, all'utente si applicherà la liberatoria del livello superiore.

Per personalizzare la priorità delle liberatorie:

1. Selezionare **Gestione posta elettronica > Liberatorie**.

2. Per modificare la priorità della liberatoria, fare clic sul pulsante accanto ad essa (su) per assegnare una priorità superiore o fare clic sul pulsante (giù) per impostarne una inferiore.

9.2 Risposte automatiche

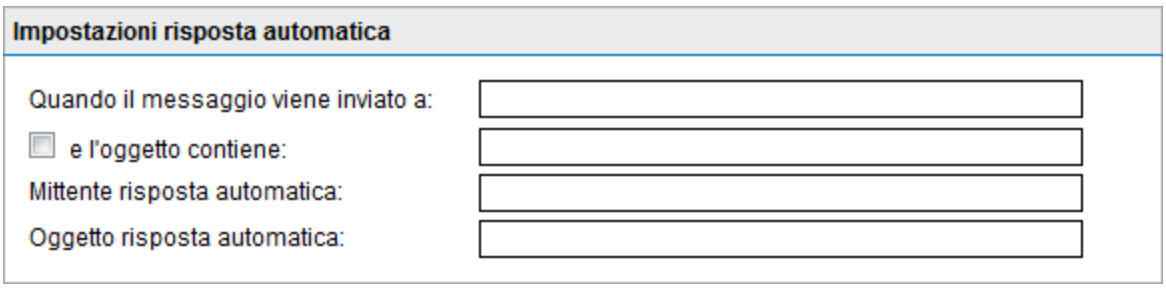
Le risposte automatiche consentono l'invio di risposte automatizzate a messaggi in entrata specifici. È possibile indicare una risposta automatica diversa per ciascun indirizzo di posta elettronica o oggetto. Per personalizzare i messaggi, è anche possibile utilizzare le variabili nelle risposte automatiche.

Per abilitare le risposte automatiche, selezionare **Gestione posta elettronica > Risposte automatiche** e selezionare **Abilita risposte automatiche**.

9.2.1 Configurazione risposte automatiche

1. Selezionare **Gestione posta elettronica > Risposte automatiche**.

2. Fare clic su **Aggiungi risposta automatica**.



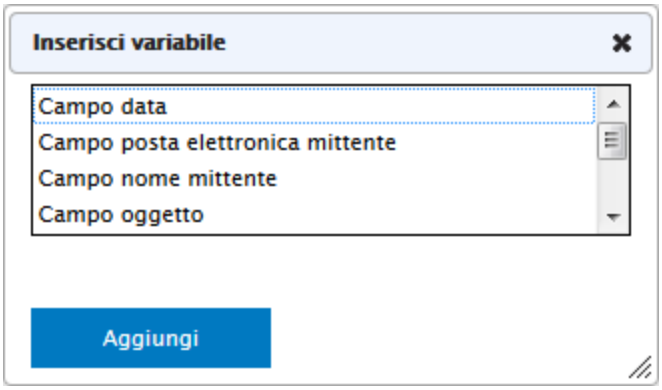
Schermata 124: impostazioni risposta automatica

3. In **Impostazioni risposta automatica**, configurare le opzioni seguenti:

Opzione	Descrizione
Quando il messaggio viene inviato a:	Digitare l'indirizzo di posta elettronica che invia risposte automatiche al momento di ricevere i messaggi. **Esempio**: se si utilizza 'vendite@dominio-master.com' i mittenti che inviano messaggi a questo indirizzo riceveranno una risposta automatica.
e l'oggetto contiene:	Questa opzione consente di abilitare le risposte automatiche per i messaggi contenenti un testo specifico nel campo dell'oggetto.
Mittente risposta automatica:	Indicare un indirizzo di posta qualora sia necessaria una risposta automatica da un indirizzo di posta diverso da quello a cui era indirizzato il messaggio in arrivo.
Oggetto risposta automatica:	Indicare l'oggetto del messaggio di risposta automatica.

4. Nel campo **Testo risposta automatica**, indicare il testo da visualizzare nel messaggio di risposta automatica.

> **NOTA**
> Importare il testo di risposta automatica da un file di testo tramite il pulsante **Importa**. Per scaricare il testo di risposta automatica in un file di testo, fare clic su **Esporta**.



Schermata 125: finestra di dialogo Variabili

5. Per personalizzare le risposte automatiche tramite variabili, fare clic su **Variabile...**. Selezionare il campo della variabile da inserire, quindi fare clic su **OK**. Le variabili disponibili sono:

Opzione	Descrizione
Campo data	Inserice la data di invio del messaggio.
Campo posta elettronica mittente	Inserisce l'indirizzo di posta elettronica del mittente.
Campo nome mittente	Inserisce il nome visualizzato del mittente.
Campo oggetto	Inserisce l'oggetto del messaggio.
Campo posta elettronica destinatario	Inserisce l'indirizzo di posta elettronica del destinatario.
Campo nome destinatario	Inserisce il nome visualizzato del destinatario.
Numero di tracciabilità	Inserisce il numero di tracciabilità (se generato).

6. Nell'area **Allegati**, selezionare gli allegati da inviare con il messaggio di risposta automatica. Specificare la posizione dell'allegato e fare clic su **Aggiungi**. Rimuovere gli allegati facendo clic su **Rimuovi**.

7. In **Altre impostazioni**, configurare:

Opzione	Descrizione
Genera numero di tracciabilità nell'oggetto	Genera un numero di tracciabilità unico nelle risposte automatiche. Per impostazione predefinita, i numeri di tracciabilità sono generati nel formato seguente: `ME_AAMMGG_nnnnnn` Dove: » `ME` : tag di GFI MailEssentials. » `AAMMGG` : data nel formato anno, mese e data. » `nnnnnn` : numero di tracciabilità generato automaticamente.
Includi messaggi inviati	Selezionare questa opzione per citare il messaggio di posta in entrata nella risposta automatica.

8. Fare clic su **Applica**.

9.3 Server elenco

I server di elenco consentono la creazione di due tipi di elenchi di distribuzione:

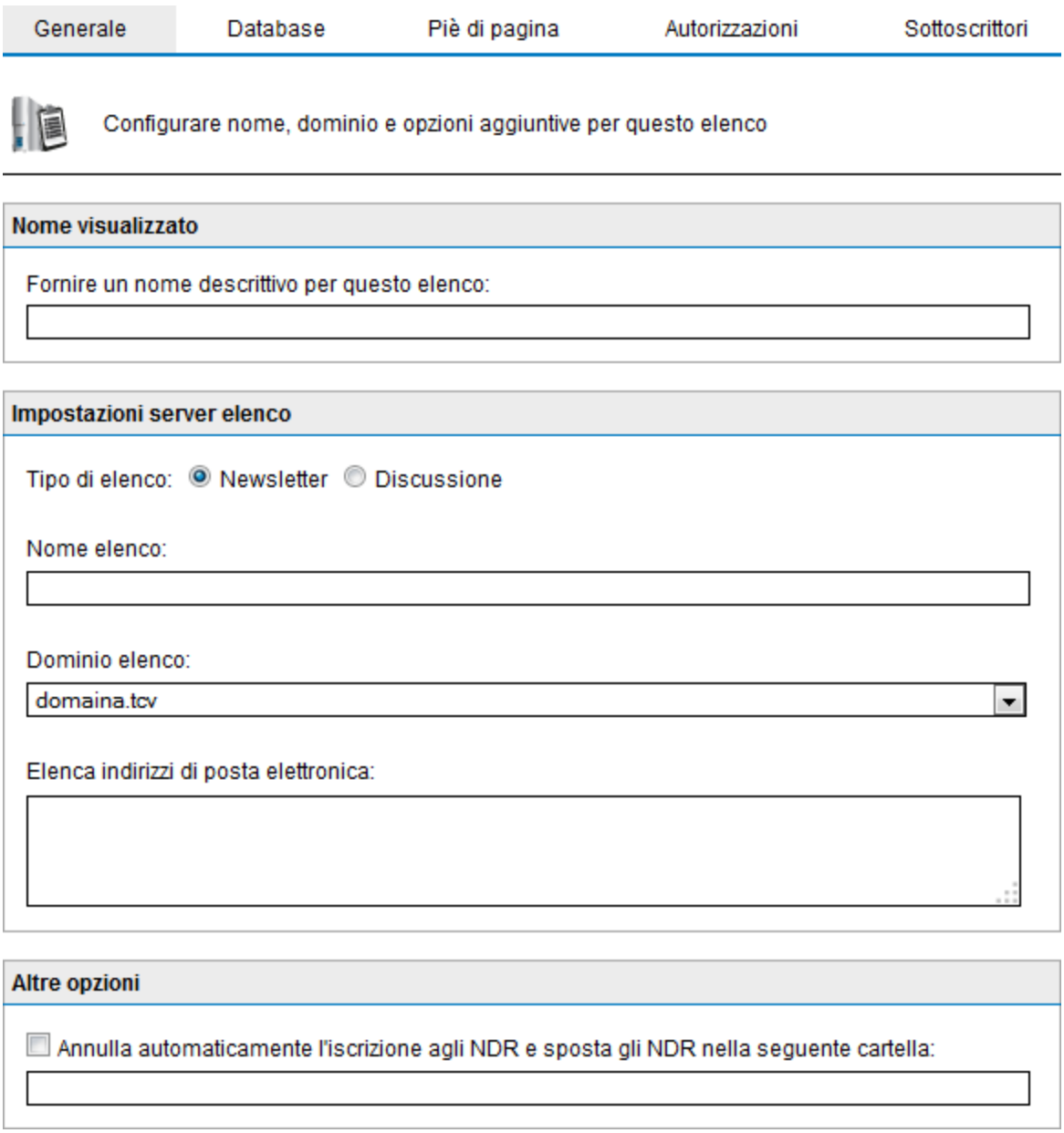
» **Newsletter**: utilizzata per la creazione di elenchi di sottoscrizione per le newsletter aziendali o di prodotti, a cui gli utenti possono iscriversi o annullare la sottoscrizione.

» **Discussione**: consente a gruppi di persone di tenere discussioni via posta elettronica, in cui ogni membro dell'elenco riceve i messaggi inviati dagli altri utenti.

9.3.1 Creazione di una newsletter o di un elenco di discussione

Per creare una nuova newsletter o un elenco di discussione:

1. Selezionare **Gestione posta elettronica > Server elenco** e fare clic su **Aggiungi elenco**.



Schermata 126: creazione di un nuovo elenco

2. Configurare le opzioni seguenti:

Opzione	Descrizione
Nome visualizzato	Immettere un nome descrittivo per il nuovo elenco.
Tipo di elenco	Selezionare il tipo di elenco discussione da creare: » **Newsletter**: utilizzata per la creazione di elenchi di sottoscrizione per le newsletter aziendali o di prodotti, a cui gli utenti possono iscriversi o annullare la sottoscrizione. » **Discussione**: consente a gruppi di persone di tenere discussioni via posta elettronica, in cui ogni membro dell'elenco riceve i messaggi inviati dagli altri utenti.
Nome elenco	Il nome dell'elenco viene utilizzato nei campi indirizzo e-mail dell'elenco. Ad esempio, se il nome elenco è `MiaNewsletter`, l'indirizzo e-mail dell'elenco sarà `MiaNewsLetter@miodominio.com`
Dominio elenco	Il dominio da utilizzare per l'elenco. L'elenco dei domini è stato estratto dall'elenco Domini locali. Il server elenco utilizza questo dominio per gli indirizzi dell'elenco visualizzati nella casella **Indirizzi e-mail elenco**.
Annulla automaticamente l'iscrizione agli NDR e sposta gli NDR nella seguente cartella:	Quando si riceve un NDR da un sottoscrittore all'elenco, viene automaticamente annullata l'iscrizione del sottoscrittore all'elenco e l'NDR viene spostato in una cartella personalizzata.

3. Dalla scheda **Database**, selezionare **Microsoft Access** o **Microsoft SQL Server/MSDE** come tipo di database. Configurare il tipo di database selezionato per memorizzare la newsletter/elenco sottoscrittori. Le opzioni disponibili sono:

Opzione	Descrizione
Microsoft Access	Specificare un nome e un percorso per il database. GFI MailEssentials creerà automaticamente un database.
Microsoft SQL Server	Indicare il nome del server SQL, le credenziali del database e di accesso utilizzate per la memorizzazione della newsletter/elenco di discussione sottoscrittori. Fare clic su Test per assicurarsi che GFI MailEssentials possa connettersi con il Microsoft SQL Server specificato.

> **NOTA**
> Per gli elenchi fino a 5000 membri, è possibile utilizzare Microsoft Access.

4. Personalizzare l'elenco di distribuzione. Per ulteriori informazioni, fare riferimento a Configurazione proprietà avanzate newsletter/elenco discussione (pagina 235).

5. Fare clic su **Applica**.

9.3.2 Utilizzo di newsletter/discussioni

Dopo aver creato una newsletter/elenco discussione, per poterne far parte, gli utenti devono effettuarvi l'iscrizione.

Azione	Descrizione
Iscrizione all'elenco	Chiedere agli utenti di inviare un messaggio a `<nomenewsletter>-subscribe@dominiopersonale.com`

Azione	Descrizione
Completare la procedura di iscrizione	Al ricevimento della richiesta, il server elenco restituisce un messaggio di conferma. Per essere aggiunti alla lista, gli utenti devono confermare l'iscrizione con un messaggio di risposta. **NOTA:** Il messaggio di conferma è obbligatorio e non può essere disattivato.
Invio di un post nella newsletter/discussione	I membri autorizzati a inviare messaggi all'elenco devono inviare il messaggio all'indirizzo relativo dell'elenco newsletter: `<nomenewsletter>@dominiopersonale.com`
Anullamento iscrizione all'elenco	Per annullare l'iscrizione all'elenco, inviare un messaggio a: `<nomenewsletter>-unsubscribe@dominiopersonale.com`

> **NOTA**
> Per consentire agli utenti di iscriversi facilmente alle newsletter, aggiungere un modulo web che chiede loro nome e indirizzo di posta e generare automaticamente un messaggio dove il mittente è l'indirizzo di posta del nuovo utente e il destinatario è:
> `<nomenewsletter>-subscribe@dominiopersonale.com`

9.3.3 Configurazione proprietà avanzate newsletter/elenco discussione

Dopo aver creato un nuovo elenco, si possono configurare opzioni aggiuntive che consentono la personalizzazione degli elementi e del comportamento dell'elenco. Queste opzioni comprendono:

- Creazione di un piè di pagina personalizzato per l'elenco
- Impostazione delle autorizzazioni per l'elenco
- Aggiunta manuale di sottoscrittori all'elenco
- Importazione di sottoscrittori nell'elenco/struttura database

Creazione di un piè di pagina personalizzato per l'elenco

1. Dalla scheda **Piè di pagina**, configurare un piè di pagina personalizzato per l'elenco discussione. Il piè di pagina viene aggiunto a ciascun messaggio inviato all'elenco.

2. Per aggiungere una versione HTML del piè di pagina, utilizzare l'editor HTML. Per aggiungere variabili al piè di pagina dell'elenco, selezionare **Inserisci > Variabili**. Scegliere la variabile da aggiungere, quindi fare clic su **Aggiungi elenco**.

3. È anche possibile inserire un piè di pagina in testo normale per gli elenchi in testo normale. Per aggiungere campi alla varabile, fare clic su **Variabile…**.

4. Fare clic su **Applica**.

> **Suggerimento**
> È possibile utilizzare i piè di pagina per mostrare le modalità a disposizione degli utenti per la sottoscrizione e l'annullamento della sottoscrizione dall'elenco e/o per promuovere i propri canali di social media.

Impostazione autorizzazioni alle newsletter

Indicare gli utenti che possono inviare newsletter.

NOTA
Le autorizzazioni non sono configurabili per gli elenchi di discussione.

1. Aprire un elenco esistente o crearne uno nuovo e accedere alla scheda **Autorizzazioni**.

2. Digitare un indirizzo e-mail che può inviare newsletter e fare clic su **Aggiungi e-mail**. L'indirizzo e-mail viene aggiunto all'elenco.

3. La password della newsletter protegge l'accesso alle newsletter qualora qualcun altro sfrutti il client di posta elettronica o i dati account di un utente autorizzato. Abilitare le password selezionando la casella di controllo **Password obbligatoria:** e indicando la password.

NOTA
Quando si inviano messaggi alla newsletter, gli utenti devono autenticarsi includendo la password nel campo oggetto del messaggio. Le password devono essere indicate nel campo dell'oggetto come segue:
`[PASSWORD:<password>] <oggetto dell'e-mail>`
Esempio: `[PASSWORD:fammipubblicare]Offerta speciale.`
Se la password è corretta, il server elenco rimuove in automatico i dati della password dall'oggetto e inoltra il messaggio alla newsletter.

4. Fare clic su **Applica**.

Aggiunta manuale di sottoscrittori all'elenco

Aggiunta manuale di utenti a newsletter/elenchi di discussione senza alcuna azione da parte degli stessi.

NOTA
È fortemente consigliato che gli utenti si iscrivano all'elenco inviando un messaggio all'indirizzo di sottoscrizione alla newsletter/discussione. Assicurarsi di disporre dell'autorizzazione degli utenti, prima di aggiungerli manualmente all'elenco.

1. Aprire un elenco esistente o crearne uno nuovo e accedere alla scheda **Sottoscrittori**.

2. Immettere i dati del sottoscrittore nel campo **Indirizzo e-mail** (obbligatorio), **Nome**, **Cognome** e **Azienda**, quindi fare clic **Aggiungi e-mail**. L'indirizzo e-mail del nuovo sottoscrittore viene aggiunto all'elenco.

3. Per rimuovere gli utenti dalla tabella dell'elenco sottoscrittori nel momento in cui annullano l'iscrizione all'elenco (non contrassegnarli semplicemente come iscrizione annullata), selezionare la casella di controllo **Quando un utente annulla la propria iscrizione, eliminarlo dal database**.

4. Fare clic su **Applica**.

Importazione di sottoscrittori nell'elenco/struttura database

Quando viene creata una nuova newsletter o elenco di discussione, viene realizzata nel database una tabella denominata 'listname_subscribers' con i seguenti campi.

Per importare i dati nell'elenco, popolare il database con i dati necessari nei campi di seguito riportati.

Nome campo	Tipo	Valore predefinito	Contrassegni	Descrizione
Ls_id	Varchar(100)		PK	ID sottoscrittore
Ls_first	Varchar(250)			Nome
Ls_last	Varchar(250)			Cognome
Ls_email	Varchar(250)			E-mail
Ls_unsubscribed	Int	0	NOT NULL	Contrassegno Annulla sottoscrizione
Ls_company	Varchar(250)			Nome azienda

9.4 Monitoraggio posta elettronica

Il monitoraggio della posta consente la copia dei messaggi inviati a o provenienti da un indirizzo di posta specifico a un altro. Ciò consente la creazione di un archivio centrale per le comunicazioni di posta per persone o reparti specifici.

9.4.1 Aggiunta di nuove regole di monitoraggio posta elettronica

1. Selezionare **Gestione posta elettronica > Monitoraggio posta elettronica**.
2. Fare clic su **Aggiungi regola...**.
3. Dalla scheda **Generale** configurare le seguenti opzioni:

Opzione	Descrizione
Nome monitor posta elettronica	Immettere un nome descrittivo per la regola monitoraggio posta elettronica.
In ingresso o **in uscita**	Selezionare se applicare la regola ai messaggi in ingresso o in uscita.
Invia una copia dei messaggi monitorati all'utente o all'indirizzo e-mail	L'indirizzo di posta elettronica di destinazione o la cassetta postale in cui copiare i messaggi. Selezionare **Indirizzo e-mail** per digitare manualmente l'indirizzo e-mail oppure selezionare **Utente** per eseguire la ricerca
Se il mittente è	Specificare l'indirizzo di posta elettronica del mittente da monitorare. Per monitorare tutte le e-mail inviate da tutti gli utenti, fare clic su**Tutti i domini**.
e il destinatario è	Specificare l'indirizzo di posta elettronica del destinatario da monitorare. Per monitorare le e-mail ricevute da tutti gli utenti, fare clic su **Tutti i domini**.

4. Fare clic su **Aggiungi** per aggiungere la regola configurata.
5. Per specificare filtri multipli, ripetere i passaggi precedenti.
6. Dalla scheda **Eccezioni**, specificare gli utenti e gli indirizzi e-mail a cui la regola non si applicherà. Le opzioni disponibili sono:

Opzione	Descrizione
Tranne se il mittente è	Esclude i mittenti specificati dal monitoraggio della posta. Per le regole di monitoraggio in entrata, immettere gli indirizzi e-mail non locali. Per le regole di monitoraggio in uscita, tutti gli indirizzi di questo elenco sono locali. Per cercare gli indirizzi e-mail locali, fare clic su **Cerca utente** e poi su **Aggiungi**.

Opzione	Descrizione
Tranne se il destinatario è	Esclude i destinatari specificati dall'elenco. Per le regole di monitoraggio in entrata, tutti gli indirizzi di questo elenco sono locali. Per cercare gli indirizzi e-mail locali, fare clic su **Cerca utente** e poi su **Aggiungi**. Per le regole di monitoraggio in uscita, immettere gli indirizzi e-mail non locali.

7. Fare clic su **Applica**.

9.4.2 Modalità d'uso di monitoraggio posta elettronica

Per informazioni su come configurare il monitoraggio della posta elettronica per i vari requisiti e scenari, fare riferimento alla tabella sottostante:

Oggetto del monitoraggio	Descrizione
Tutta la posta inviata da un utente specifico	Creare una regola in uscita e indicare l'e-mail del mittente o scegliere l'utente (se si utilizza AD) dal campo mittente. Nel campo del destinatario, fare clic su **Tutti i domini**.
Tutta la posta inviata a un utente specifico	Creare una regola in entrata e indicare l'indirizzo e-mail del destinatario o scegliere l'utente (se si utilizza AD) dal campo destinatario. Nel campo del mittente, fare clic su **Tutti i domini**.
Posta inviata da un utente specifico a un destinatario esterno	Creare una regola in uscita, indicare il mittente o scegliere l'utente (se si utilizza AD) dal campo mittente. Digitare l'indirizzo di posta del destinatario nel campo apposito.
Posta inviata a un utente specifico da un mittente esterno	Creare una regola in entrata e indicare l'indirizzo di posta del mittente esterno nel campo apposito. Indicare l'indirizzo e-mail o scegliere l'utente (se si utilizza AD) dal campo destinatario.
Posta inviata da un utente specifico a un'azienda o dominio	Creare una regola in uscita e indicare il mittente o scegliere l'utente (se si utilizza AD) dal campo mittente. Indicare il dominio dell'azienda nel campo destinatario.
Posta inviata a un utente specifico da un'azienda o dominio	Creare una regola in entrata e indicare il dominio dell'azienda nel campo del mittente. Selezionare il dominio facendo clic sul pulsante del mittente e immettere il nome utente o l'indirizzo di posta dell'utente nel campo del destinatario.

9.4.3 Abilitazione/disabilitazione regole monitoraggio posta elettronica

1. Selezionare **Gestione posta elettronica > Monitoraggio posta elettronica**.

2. Selezionare la regola da abilitare/disabilitare.

3. Per abilitare o disabilitare rispettivamente la regola selezionata, fare clic su **Abilita selezionati** o **Disabilita selezionati**.

4. Fare clic su **OK** per salvare le modifiche.

10 Impostazioni generali

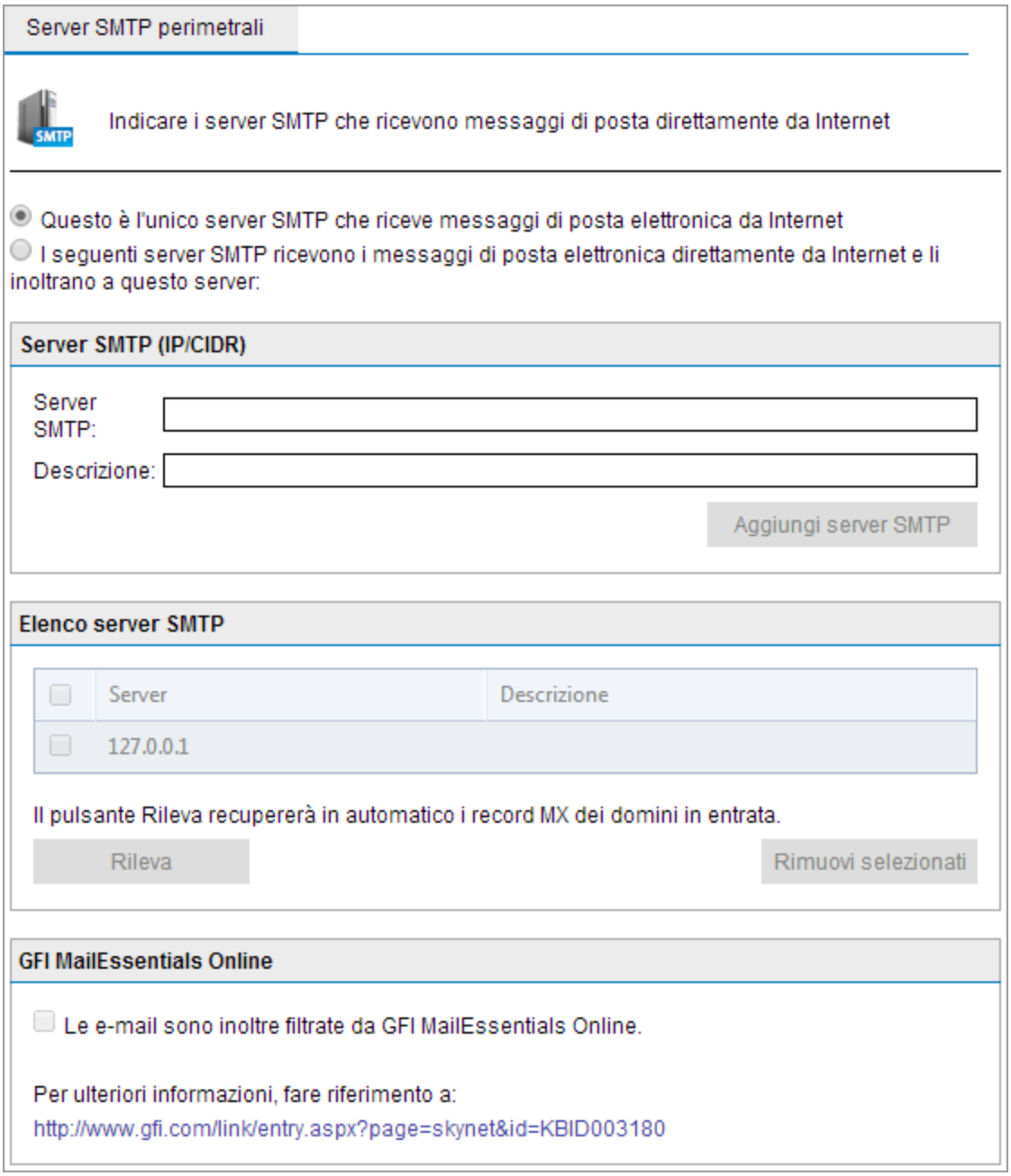
Argomenti del presente capitolo:

10.1 Indirizzo e-mail amministratore 241
10.2 Abilitazione/disabilitazione dei moduli di scansione 241
10.3 Impostazioni proxy 242
10.4 Domini locali 244
10.5 Gestione utenti locali 245
10.6 Gestione licenze 246
10.7 Binding server virtuale SMTP 246
10.8 Controllo patch 247
10.9 Controllo di accesso 248

10.0.1 Impostazioni server SMTP perimetrali

È necessario specificare i server SMTP che inoltrano i messaggi al server GFI MailEssentials.

1. Dalla configurazione di GFI MailEssentials, andare a **Impostazioni generali > Server SMTP perimetrali**.


Server SMTP perimetrali
Indicare i server SMTP che ricevono messaggi di posta direttamente da Internet
Questo è l'unico server SMTP che riceve messaggi di posta elettronica da Internet
I seguenti server SMTP ricevono i messaggi di posta elettronica direttamente da Internet e li inoltrano a questo server:
Server SMTP (IP/CIDR)
Server SMTP:
Descrizione:
Aggiungi server SMTP
Elenco server SMTP
Server
Descrizione
127.0.0.1
Il pulsante Rileva recupererà in automatico i record MX dei domini in entrata.
Rileva
Rimuovi selezionati
GFI MailEssentials Online
Le e-mail sono inoltre filtrate da GFI MailEssentials Online.
Per ulteriori informazioni, fare riferimento a:
http://www.gfi.com/link/entry.aspx?page=skynet&id=KBID003180

Schermata 127: impostazioni server SMTP perimetrali

2. Configurare le opzioni seguenti:

Opzione	Descrizione
Questo è l'unico server SMTP che riceve messaggi di posta elettronica da Internet	Scegliere questa opzione se GFI MailEssentials è installato sull'unico server SMTP che riceve messaggi di posta esterni direttamente da Internet.
I seguenti server SMTP ricevono i messaggi di posta elettronica direttamente da Internet e li inoltrano a questo server.	I messaggi di posta vengono inoltrati al server GFI MailEssentials da altri server SMTP. Aggiungere questi server SMTP all'elenco server SMTP: **Rilevazione automatica:** per rilevare in automatico i server SMTP recuperando i record MX dei domini in entrata, fare clic su **Rileva**. **Aggiunta manuale:** Per aggiungere manualmente gli indirizzi IP dei server SMTP che inoltrano messaggi al server di GFI MailEssentials, digitare l'indirizzo IP o un intervallo di indirizzi IP (utilizzando la notazione CIDR), quindi fare clic su **Aggiungi server SMTP**.

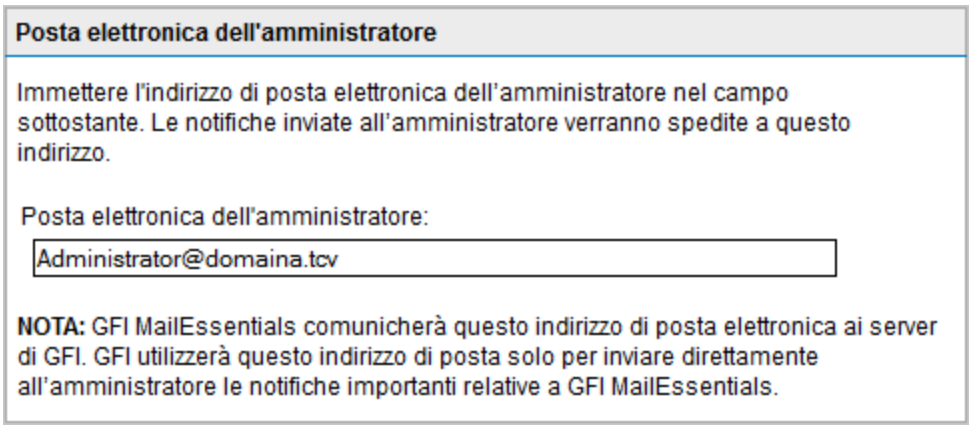
Opzione	Descrizione
Le e-mail sono inoltre filtrate da GFI MailEssentials Online	Selezionare questa opzione se si utilizzano il prodotto di sicurezza e-mail in hosting GFI MailEssentials Online. per ulteriori informazioni, fare riferimento a: http://go.gfi.com/?pageid=ME_MAXMPME

3. Fare clic su **Applica**.

10.1 Indirizzo e-mail amministratore

GFI MailEssentials invia importanti notifiche all'amministratore via posta elettronica. Per configurare l'indirizzo di posta elettronica dell'amministratore:

1. Da GFI MailEssentials Configuration, selezionare **Impostazioni generali > Impostazioni** e scegliere la scheda **Generale**.


Posta elettronica dell'amministratore
Immettere l'indirizzo di posta elettronica dell'amministratore nel campo sottostante. Le notifiche inviate all'amministratore verranno spedite a questo indirizzo.
Posta elettronica dell'amministratore:
Administrator@domaina.tcv
NOTA: GFI MailEssentials comunicherà questo indirizzo di posta elettronica ai server di GFI. GFI utilizzerà questo indirizzo di posta solo per inviare direttamente all'amministratore le notifiche importanti relative a GFI MailEssentials.

Schermata 128: indicazione indirizzo e-mail amministratore

2. Digitare l'indirizzo di posta elettronica dell'amministratore nell'area **Indirizzo e-mail amministratore**.

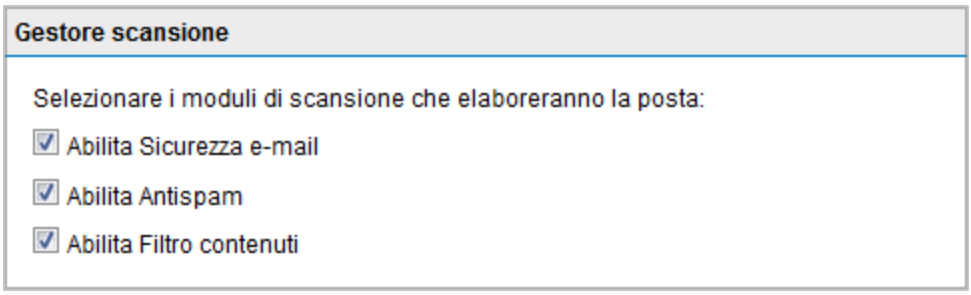
3. Fare clic su **Applica**.

10.2 Abilitazione/disabilitazione dei moduli di scansione

Da GFI MailEssentials è possibile abilitare o disabilitare moduli di scansione della posta specifici. Questo consente l'attivazione e la disattivazione dei motori di scansione o dei filtri in batch.

> **NOTA**
> Questa caratteristica abilita o disabilita solo specifici motori di scansione. I motori disabilitati non elaborano i messaggi in entrata, in uscita e/o interni. Tutte le altre funzioni di GFI MailEssentials, come quarantine store, sono ancora funzionanti.

1. Da GFI MailEssentials Configuration, selezionare **Impostazioni generali > Impostazioni** e scegliere la scheda **Generale**.



Schermata 129: Gestore scansione

2. abilitazione o disabilitazione dei moduli di scansione: abilitazione o disabilitazione dei moduli di scansione:

Opzione	Descrizione
Abilita Sicurezza e-mail	Abilitazione o disabilitazione dei seguenti motori di scansione: » Motori di scansione antivirus » Protezione archivio informazioni » Scanner trojan ed eseguibili » Motore exploit posta » Strumento di disinfezione HTML
Abilita antispam	Abilita/disabilita i seguenti filtri antispam: » SpamRazer » Antiphishing » Raccolta di directory » Block list e-mail » Block list IP » Block list DNS IP » Block list DNS URI » Sender Policy Framework » Anti-spoofing » Greylist » Rilevamento lingua » Controllo intestazione » Controllo parola chiave spam » Analisi bayesiana » Whitelist » Nuovi mittenti
Abilita filtro contenuti	Abilita/disabilita i seguenti motori di filtro contenuti: » Filtro parola chiave » Filtro allegati » Motore di decompressione » Filtro avanzato contenuto

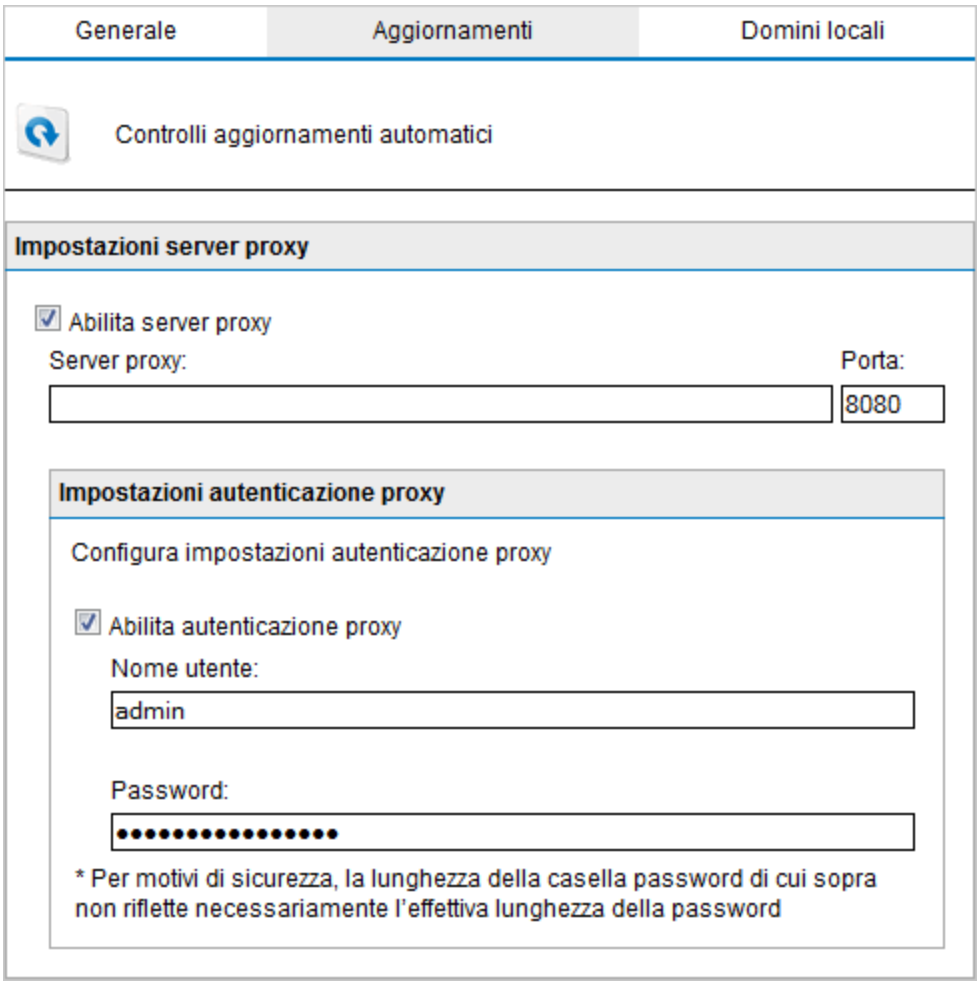
3. Fare clic su **Applica**.

10.3 Impostazioni proxy

GFI MailEssentials controlla e scarica automaticamente gli aggiornamenti (ad esempio, gli aggiornamenti delle definizioni dei virus e delle definizioni di SpamRazer) da Internet. Se il server su

cui è installato GFI MailEssentials si connette a Internet tramite server proxy, configurare come segue le impostazioni del server proxy:

1. Da GFI MailEssentials Configuration, selezionare **Impostazioni generali > Impostazioni** e fare clic sulla scheda **Aggiornamenti**.



Schermata 130: aggiorna le impostazioni del server proxy

2. Selezionare la casella di controllo **Abilita server proxy**.

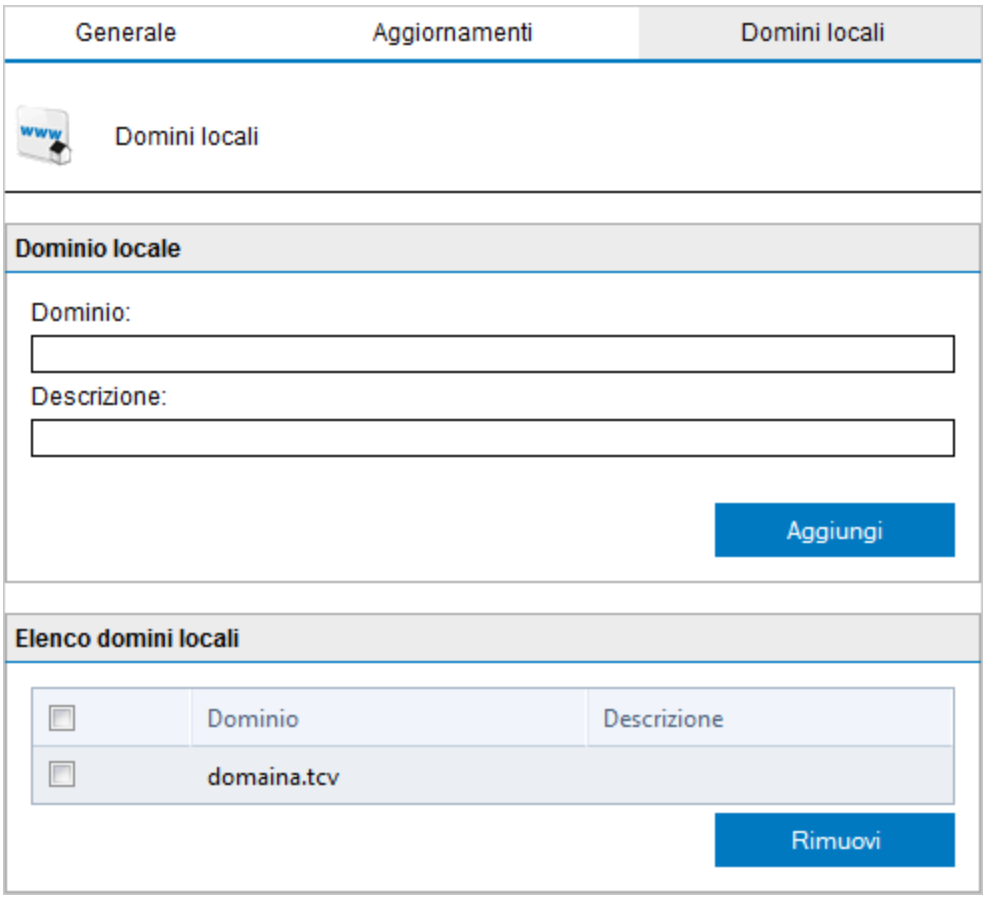
3. Nel campo **Server proxy**, inserire il nome o l'indirizzo IP del server proxy.

4. Nel campo **Porta**, digitare la porta a cui connettersi (il valore predefinito è 8080).

5. Se il server proxy richiede l'autenticazione, selezionare **Abilita autenticazione proxy** e digitare **Nome utente** e **Password**.

6. Fare clic su **Applica**.

10.4 Domini locali



Schermata 131: elenco domini locali

GFI MailEssentials richiede l'elenco di domini locali per poter distinguere tra posta in entrata, in uscita o interna. Durante la procedura di installazione o di post-installazione, GFI MailEssentials importa in automatico i domini locali dal servizio SMTP di IIS o da Microsoft® Exchange Server. In alcuni casi, tuttavia, potrebbe essere necessario aggiungere manualmente i domini locali.

IMPORTANTE
GFI MailEssentials filtra alla ricerca di spam solo i messaggi destinati ai domini locali. Alcuni filtri delle regole sono anche basati sulla direzione. Questo è determinato dai domini locali.

Per aggiungere o rimuovere i domini locali dopo l'installazione, seguire questi passaggi:

1. Selezionare **Impostazioni generali > Impostazioni** e fare clic sulla scheda **Domini locali**.

2. Digitare il nome e la descrizione del dominio da aggiungere nelle caselle di testo **Dominio** e **Descrizione**.

3. Fare clic su **Aggiungi** per includere il dominio indicato nell'elenco **Domini locali**.

NOTA
Per rimuovere un dominio elencato, selezionarlo dall'elenco e fare clic su **Rimuovi**.

4. Fare clic su **Applica**.

10.5 Gestione utenti locali

GFI MailEssentials utilizza 3 modalità per recuperare gli utenti a seconda dell'ambiente di installazione.

> **NOTA**
> Il numero degli utenti recuperato viene usato anche a scopi di licenza.

10.5.1 GFI MailEssentials è installato nella modalità Active Directory

Quando GFI MailEssentials non è installato sullo stesso computer del server di posta ed è presente Active Directory, GFI MailEssentials recupera gli utenti abilitati all'utilizzo della posta dal dominio di Active Directory di cui fa parte il computer dove è installato GFI MailEssentials.

10.5.2 GFI MailEssentials installato in un computer Microsoft® Exchange Server

Quando GFI MailEssentials è installato sullo stesso computer di Microsoft® Exchange, GFI MailEssentials recupera gli utenti di Active Directory che dispongono di una cassetta postale sullo stesso Microsoft® Exchange Server.

10.5.3 GFI MailEssentials installato in modalità SMTP

Quando si sceglie di installare GFI MailEssentials in modalità SMTP, l'elenco di utenti locali viene archiviato in un database gestito da GFI MailEssentials.

Per popolare e gestire l'elenco utenti quando GFI MailEssentials è installato in modalità SMTP, selezionare **Generale > Impostazioni** e selezionare la scheda **Gestione utenti**.

La scheda **Gestione utenti** riporta l'elenco di utenti locali e consente di aggiungere o rimuovere gli utenti locali. L'elenco di utenti locali viene utilizzato durante la configurazione delle regole basate sugli utenti, come le regole di **Filtro allegati** e di **Filtro contenuti**.

> **NOTA**
> GFI MailEssentials popola automaticamente l'elenco di utenti locali utilizzando l'indirizzo di posta del mittente nei messaggi in uscita.

Per aggiungere un nuovo utente locale:

1. Immettere l'indirizzo e-mail nella casella **Indirizzo di posta elettronica**.
2. Fare clic su **Aggiungi**.
3. Per aggiungere altri utenti locali, ripetere l'operazione e fare clic su **Applica**.

Per rimuovere un utente locale:

1. Selezionare l'utente locale da rimuovere dall'elenco **Utenti locali** e fare clic su **Rimuovi**.
2. Per rimuovere altri utenti locali, ripetere l'operazione e fare clic su **Applica**.

10.6 Gestione licenze

Acquistare una licenza equivalente al numero di cassette postali o utenti protetti da GFI MailEssentials.

Immettere il codice di licenza acquistato durante l'installazione o dalla configurazione di GFI MailEssentials. Selezionare **Impostazioni generali > Gestione licenze** e immettere la licenza nella casella **Codice di licenza**. Fare clic su **Applica**.

10.6.1 Informazioni codice di licenza

Per rivedere le informazioni sulla licenza, compresa la data di scadenza dell'abbonamento, selezionare **Impostazioni generali > Gestione licenze** e rivedere i dati in **Informazioni codice di licenza**.

Etichetta	Descrizione
Edizione prodotto	L'edizione di GFI MailEssentials dipende dal tipo di abbonamento acquistato: » **Antispam**: abilita la funzionalità di filtro antispam. I motori di scansione di sicurezza e antimalware sono disabilitati. » **EmailSecurity**: abilita i motori di scansione di sicurezza e antimalware. I filtri antispam sono disabilitati. » **UnifiedProtection**: include sia la funzionalità antispam che quella di sicurezza della posta.
Antispam	Mostra se la funzionalità antispam è dotata di licenza.
EmailSecurity	Indica se la funzione di sicurezza e antimalware è dotata di licenza.
Stato abbonamento	La data di scadenza dell'abbonamento. Quando la licenza scade, il server della posta non sarà più protetto. GFI MailEssentials interrompe la scansione delle e-mail e il download degli aggiornamenti.
Numero di utenti provvisti di licenza	Il numero massimo di utenti consentiti dalla licenza acquistata.
Numero di utenti attuale	Il numero di utenti che viene protetto da GFI MailEssentials.

10.6.2 Determinazione dei requisiti di licenza

GFI MailEssentials conta le cassette postali/indirizzi e-mail totali a seconda dell'ambiente. Per determinare il numero di utenti nel proprio ambiente, selezionare http://go.gfi.com/?pageid=ME_RetrieveAndCountUsers.

10.7 Binding server virtuale SMTP

GFI MailEssentials si collega sempre al primo server virtuale SMTP configurato in IIS. In caso di server virtuali SMTP multipli, potrebbe essere necessario associare GFI MailEssentials a un server virtuale SMTP nuovo o diverso.

> **NOTA**
> La scheda di binding del server virtuale SMTP non viene visualizzata se si è installato GFI MailEssentials su un computer con Microsoft® Exchange Server 2007/2010.

10.7.1 Binding di GFI MailEssentials a un altro server virtuale SMTP.

> **NOTA**
> Durante l'esecuzione di questa operazione, alcuni servizi vengono arrestati temporaneamente. Questo potrebbe incidere sul flusso della posta e/o la scansione della posta.

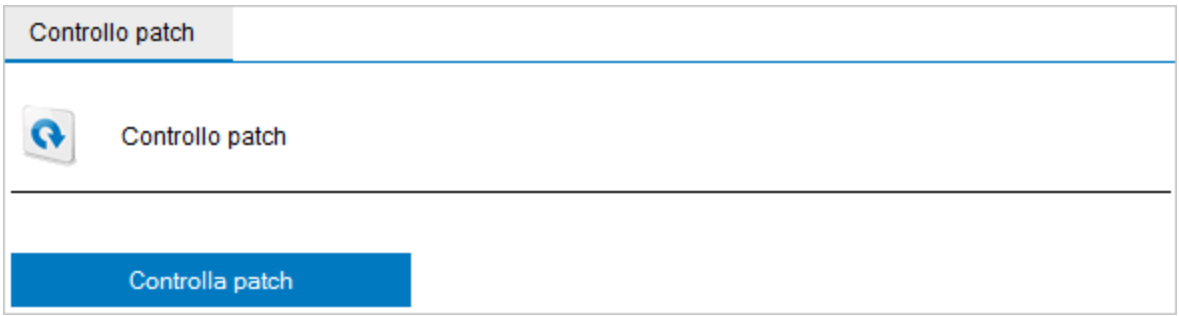
1. Selezionare **Impostazioni generali > Impostazioni** e fare clic sulla scheda **Binding**.
2. Selezionare il server virtuale SMTP da associare a GFI MailEssentials.
3. Fare clic su **Applica**.
4. GFI MailEssentials chiederà il riavvio dei servizi per rendere effettive le nuove impostazioni.

10.8 Controllo patch

La funzione Controllo patch verifica la presenza di patch software disponibili per la versione attuale di GFI MailEssentials effettuando la connessione diretta ai server di aggiornamento GFI.

> **NOTA**
> Per mantenere le patch di GFI MailEssentials aggiornate, si consiglia di effettuare la verifica periodicamente.

1. Selezionare **Impostazioni generali > Controllo patch**.



Schermata 132: controllo patch del prodotto

2. Fare clic su **Controlla patch** per eseguire la connessione al server di aggiornamento GFI e verificare gli aggiornamenti disponibili.
3. Per effettuare il download, fare clic sul collegamento **Download** delle patch.
4. Al termine del download, installare gli aggiornamenti scaricati.

> **NOTA**
> Per accedere alle istruzioni di installazione e ad altre informazioni applicabili a una patch, fare clic sul collegamento di informazioni fornito nell'elenco degli aggiornamenti disponibili. Un'installazione errata delle patch potrebbe causare l'errato funzionamento del prodotto o il peggioramento delle sue prestazioni.

10.9 Controllo di accesso

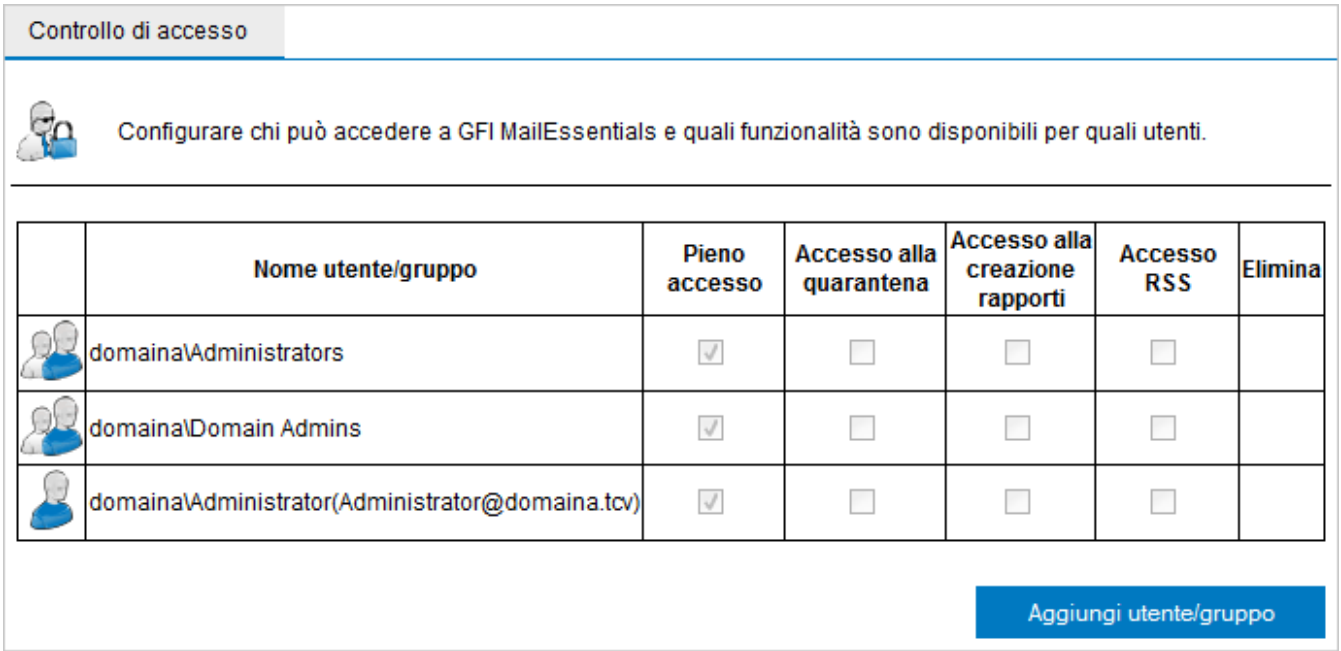
Consentire o bloccare l'accesso alle varie funzioni di GFI MailEssentials per utenti di dominio o gruppi specifici. Gli utenti possono accedere alla UI web di GFI MailEssentials tramite le loro credenziali di dominio. Le funzioni mostrate agli utenti connessi dipendono dalla configurazione di Controllo di accesso.

> **NOTA**
> La configurazione del controllo di accesso dalla UI web è possibile solo quando GFI MailEssentials viene eseguito in modalità IIS ed è possibile accedervi dalla rete. Controllo di accesso non è configurabile dalla Switchboard quando GFI MailEssentials viene eseguito in modalità locale. Per ulteriori informazioni, fare riferimento a Elenco di controllo di accesso (pagina 253).

Il gruppo **Domain admin** (solo in un ambiente Active Directory) e l'account/gruppo amministratore server riceveranno automaticamente privilegi di accesso completo a tutte le funzioni di GFI MailEssentials.

Ad altri utenti o gruppi può essere dato accesso totale o parziale a determinate funzioni di GFI MailEssentials. Per aggiungere utenti all'elenco di controllo di accesso:

1. Da GFI MailEssentials Configuration, andare a **Impostazioni generali > Controllo di accesso**. Aggiungere gli utenti o i gruppi del dominio e selezionare le funzionalità del prodotto a cui consentire l'accesso.



Schermata 133: Impostazioni Controllo di accesso

2. Fare clic su **Aggiungi utente/gruppo**.

3. Nella finestra di dialogo **Ricerche utente**, inserire il nome dell'utente o del gruppo da aggiungere, quindi fare clic su **Controlla nomi**.

4. GFI MailEssentials mostra l'elenco di utenti/gruppi individuati. Selezionare gli utenti/gruppi da aggiungere da aggiungere e fare clic su **Invia**.

5. Per gli utenti/gruppi aggiunti di recente, selezionare le funzionalità a cui consentire l'accesso.

Autorizzazione	Descrizione
Pieno accesso	L'utente può accedere e configurare tutte le funzionalità del prodotto.
Accesso alla quarantena	Consente l'accesso alla ricerca nella quarantena e alle cartelle di ricerca.
Accesso alla creazione rapporti	Consente agli utenti di generare rapporti.
Accesso RSS	Consente agli utenti di iscriversi ai feed RSS quarantena.

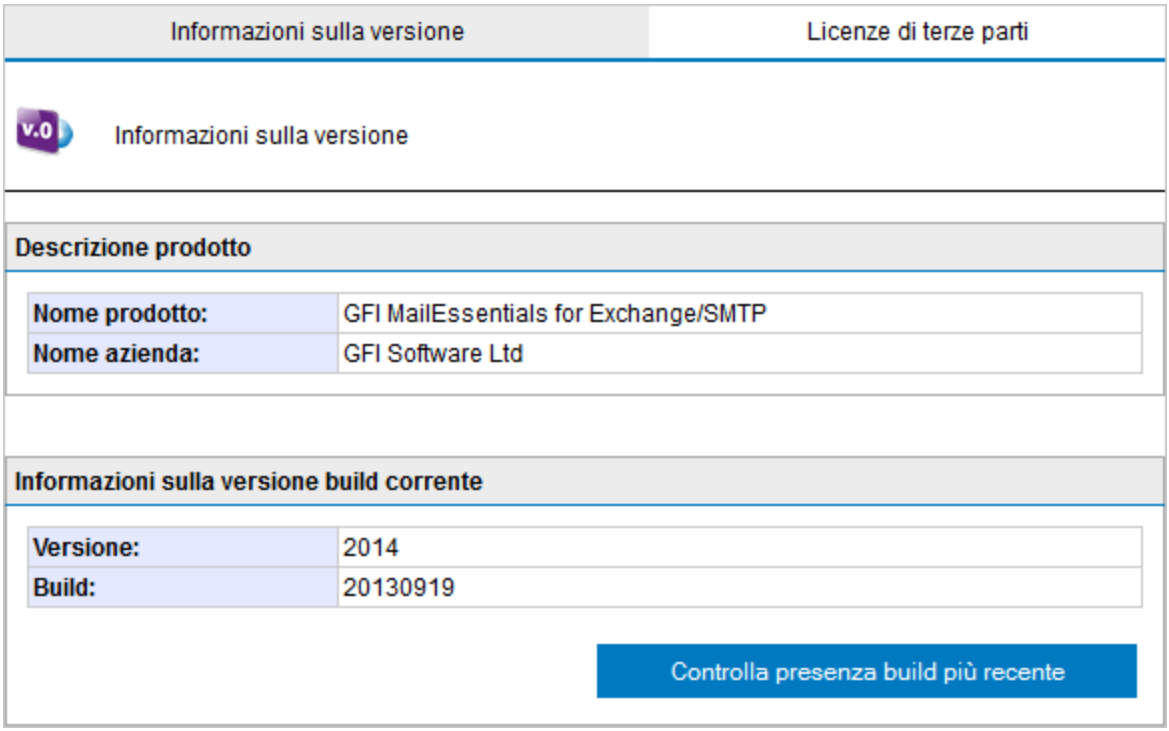
6. Fare clic su **Applica**.

11 Argomenti vari

Argomenti del presente capitolo:

11.1 Informazioni di installazione 250
11.2 Nomi directory virtuale 251
11.3 Modalità interfaccia utente 251
11.4 Messaggi di posta elettronica non riusciti 256
11.5 Analisi 258
11.6 POP2Exchange - Download messaggi dal server POP3 259
11.7 Spostamento messaggi spam nelle cartelle della cassetta postale degli utenti 263
11.8 Spostamento spam nella cartella di Exchange 2010 266
11.9 Sincronizzazione dati di configurazione 266
11.10 Disabilitazione elaborazione messaggi di posta elettronica 278
11.11 Backup posta elettronica prima e dopo l'elaborazione 279
11.12 Porte remote 280
11.13 Monitoraggio API di scansione antivirus 281

11.1 Informazioni di installazione



Schermata 134: pagina di informazioni sulla versione

Per visualizzare le informazioni sulla versione di GFI MailEssentials, selezionare il nodo **Informazioni su**. La scheda **Informazioni sulla versione** visualizza la versione e il numero di build dell'installazione di GFI MailEssentials.

Per controllare se sul computer è installata l'ultima build di GFI MailEssentials, fare clic su **Controlla presenza build più recente**.

> **NOTA**
> Al momento di contattare il supporto, citare sempre la versione di GFI e le informazioni sulla build.

La scheda **Licenze di terze parti** elenca i componenti di terze parti utilizzati da GFI MailEssentials.

11.2 Nomi directory virtuale

I nomi della directory virtuale predefinita di GFI MailEssentials e RSS Quarantena sono rispettivamente **MailEssentials** e **MailEssentialsRSS**. I nome della directory virtuale sono personalizzabili, tuttavia, è consigliabile non modificarli.

> **NOTA**
> Se GFI MailEssentials è configurato per l'accesso solo dal computer locale, la directory virtuale di GFI MailEssentials Configuration non sarà configurabile.

1. Avviare GFI MailEssentials Switchboard da **Start > Tutti i programmi > GFI MailEssentials > Switchboard**.

2. Dall'area **Opzioni modalità interfaccia utente IIS**, indicare i nomi personalizzati della directory virtuale per:

» GFI MailEssentials Configuration: digitare un nome personalizzato nel campo **Directory virtuale**.

» Directory virtuale RSS di quarantena: digitare un nome personalizzato nel campo **Directory virtuale RSS**.

3. Fare clic su **Applica**.

4. Fare clic su **OK** e attendere l'applicazione delle nuove impostazioni.

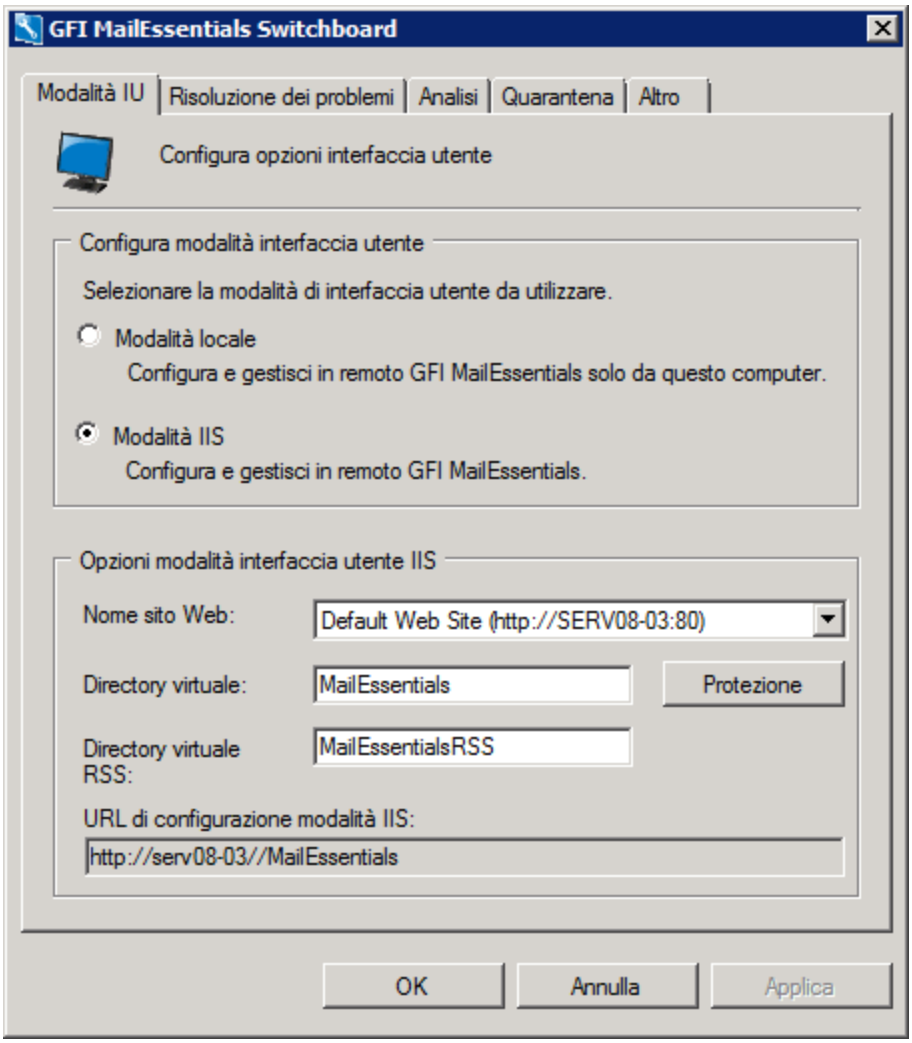
5. Una volta completato il processo, fare clic su **OK**.

11.3 Modalità interfaccia utente

L'interfaccia utente di GFI MailEssentials può essere caricata solo sul computer di installazione (modalità locale) o accessibile sulla rete tramite http (modalità IIS).

Per selezionare la modalità:

1. Avviare GFI MailEssentials Switchboard da **Start > Tutti i programmi > GFI MailEssentials > Switchboard**.



Schermata 135: GFI MailEssentials switchboard - Modalità IU

2. Dall'area **Modalità IU**, selezionare:

Opzione	Descrizione
Modalità locale	GFI MailEssentials carica in un'applicazione visualizzatore html, accessibile solo dal computer dove è installato GFI MailEssentials. **NOTA** Se si utilizza la modalità locale: » I collegamenti dei digest spam non funzioneranno » Il portale utente non sarà disponibile, gli utenti non potranno gestire le whitelist e blocklist personali e la loro quarantena personale. Per ulteriori informazioni, fare riferimento a Azioni utente finale (pagina 21).
Modalità IIS (consigliata)	GFI MailEssentials carica nel browser web predefinito utilizzando le impostazioni di installazione di IIS configurate durante l'installazione. Anche l'interfaccia utente è accessibile sulla rete tramite http. **NOTA** Le impostazioni di configurazione di IIS possono essere modificate dai campi nome del sito web, directory virtuale e directory virtuale RSS. Le opzioni di **Protezione** consentono la configurazione di un elenco di controllo di accesso e dell'autenticazione IIS.

NOTA

Durante l'esecuzione di questa operazione, alcuni servizi vengono arrestati temporaneamente. Questo potrebbe incidere sul flusso della posta e/o la scansione della posta.

3. Per eseguire il riavvio dei servizi visualizzati, fare clic su **Sì**.

4. Fare clic su **OK**.

11.3.1 Impostazioni protezione IIS

Il pulsante **Protezione** all'interno della scheda Modalità IU consente la configurazione di un elenco di controllo di accesso e di un metodo di autenticazione.

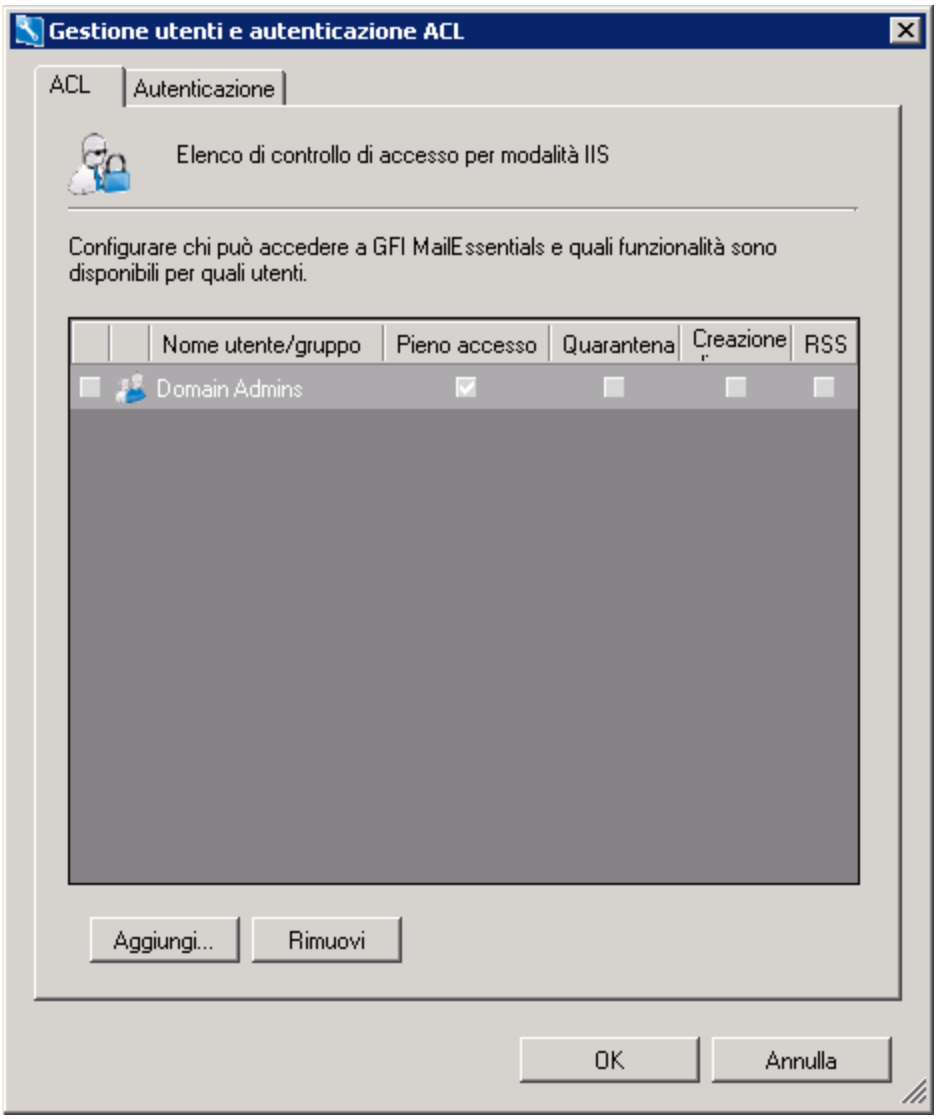
Elenco di controllo di accesso

L'elenco di controllo di accesso indica chi può accedere a GFI MailEssentials e quali funzionalità sono disponibili per quali utenti o gruppi. Per impostazione predefinita, gli amministratori dispongono di accesso completo a GFI MailEssentials, tuttavia è possibile indicare utenti o gruppi specifici con tipi di accesso differenti.

Per aggiungere un utente:

1. Caricare la Switchboard facendo clic su **Start > Tutti i programmi >GFI MailEssentials > Switchboard**.

2. Selezionare la scheda **Modalità IU**. Fare clic su **Modalità IIS** e selezionare **Protezione**.



Schermata 136: protezione IIS - Scheda ACL

3. Fare clic su **Aggiungi...** e inserire il nome dell'utente o del gruppo da aggiungere all'elenco.

4. Selezionare il tipo di accesso da assegnare. Le opzioni disponibili sono:

Autorizzazione	Descrizione
Pieno accesso	L'utente può accedere e configurare tutte le funzionalità del prodotto.
Accesso alla quarantena	Consente l'accesso alla ricerca nella quarantena e alle cartelle di ricerca.
Accesso alla creazione rapporti	Consente agli utenti di generare rapporti.
Accesso RSS	Consente agli utenti di iscriversi ai feed RSS quarantena.

5. Per finalizzare le impostazioni, fare clic su **OK**.

Per rimuovere l'accesso a un utente o a un gruppo, selezionare l'elemento da rimuovere e fare clic su **Rimuovi**.

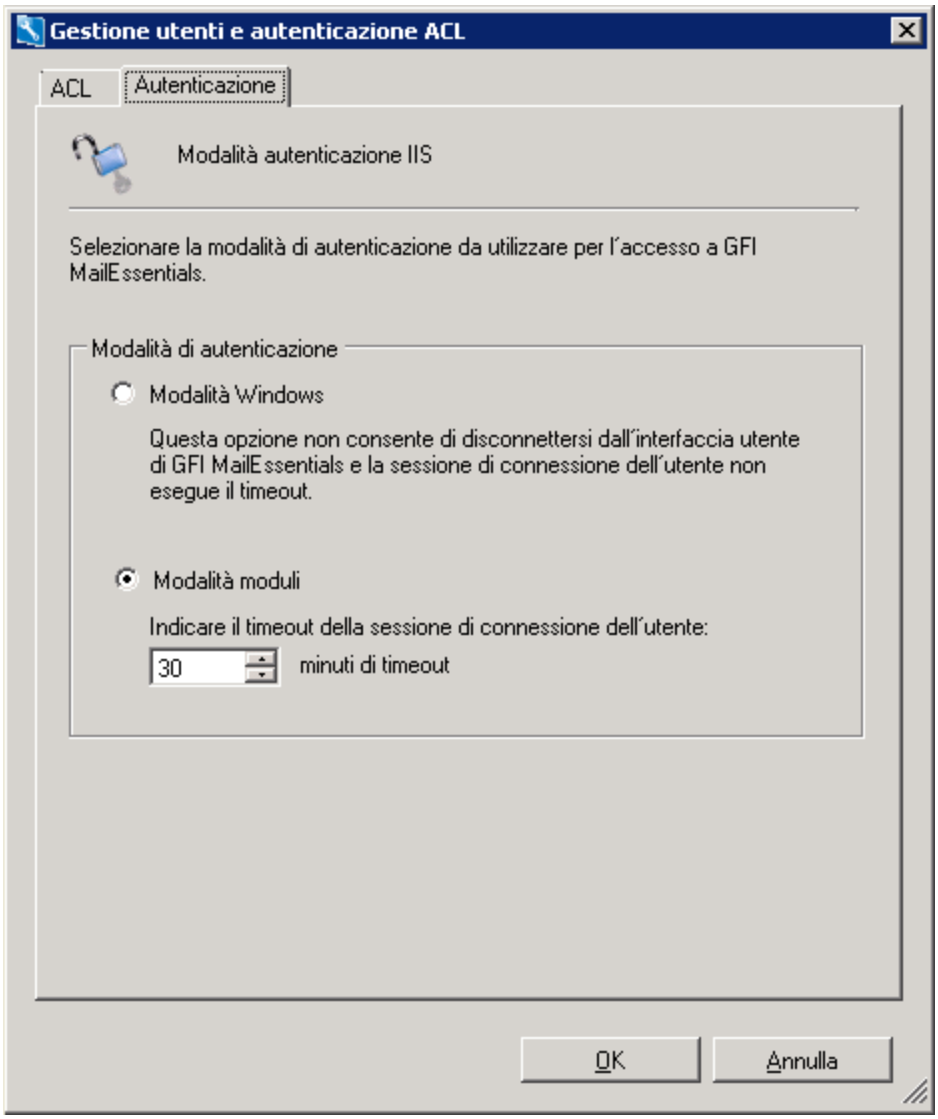
Modalità autenticazione IIS

La modalità autenticazione IIS consente di scegliere il metodo di autenticazione da utilizzare per l'accesso a GFI MailEssentials.

1. Caricare la Switchboard facendo clic su **Start > Tutti i programmi >GFI MailEssentials > Switchboard**.

2. Selezionare la scheda **Modalità IU**. Fare clic su **Modalità IIS** e selezionare **Protezione**.

3. Selezionare la scheda **Autenticazione**.


Gestione utenti e autenticazione ACL
ACL
Autenticazione
Modalità autenticazione IIS
Selezionare la modalità di autenticazione da utilizzare per l'accesso a GFI MailEssentials.
Modalità di autenticazione
Modalità Windows
Questa opzione non consente di disconnettersi dall'interfaccia utente di GFI MailEssentials e la sessione di connessione dell'utente non esegue il timeout.
Modalità moduli
Indicare il timeout della sessione di connessione dell'utente:
30
minuti di timeout
OK
Annulla

Schermata 137: protezione IIS - scheda Autenticazione

4. Selezionare una delle opzioni disponibili:

Opzione	Descrizione
Modalità Windows	L'autenticazione Windows consente a GFI MailEssentials di utilizzare le credenziali dell'utente attualmente connesso e non offre la disconnessione e il timeout automatico della sessione dell'interfaccia utente.
Modalità moduli	(Predefinita) L'autenticazione moduli consente agli utenti di disconnettersi. Permette inoltre di configurare un timeout automatico dalla sessione dell'interfaccia utente. Questa opzione è consigliata se gli utenti finali accedono alla loro console utenti di GFI MailEssentials, soprattutto da computer pubblici.

5. Fare clic su **OK** per salvare le impostazioni.

11.4 Messaggi di posta elettronica non riusciti

Possono esserci delle istanze dove i filtri di sicurezza e-mail o dei contenuti di GFI MailEssentials non riescono a scansionare un messaggio, ad esempio i messaggi con informazioni dell'intestazione danneggiate. In questo caso, GFI MailEssentials blocca il messaggio per la probabile presenza di contenuto dannoso e lo sposta nella cartella seguente:

<GFI MailEssentials percorso di installazione>\EmailSecurity\failedmails

11.4.1 Rielaborazione messaggi attendibili non riusciti

È consigliabile contattare il Supporto GFI quando una serie di messaggi viene spostata nella cartella **failedmails**. Una volta risolto il problema, i messaggi possono essere nuovamente scansionati da GFI MailEssentials per determinare se è possibile consegnarli in modo sicuro.

> **NOTA**
> I file con l'estensione .PROP presenti nella cartella **failedmails** vengono utilizzati per la risoluzione dei problemi. Durante la rielaborazione dei messaggi non riusciti, questi file possono essere eliminati.

GFI MailEssentials installato in Microsoft® Exchange Server 2007/2010.

1. Nella cartella **failedmails**, modificare l'estensione dei file .TXT in .EML.

> **NOTA**
> Per cambiare automaticamente l'estensione di tutti i file .TXT presenti nella cartella **failedmails** in .EML, dal prompt dei comandi modificare la directory con la cartella **failedmails** ed eseguire il comando seguente:
> `ren *.txt *.eml`

2. Spostare i file rinominati dalla quarantena alla seguente cartella:

<unit>\Program Files\Microsoft\Exchange Server\TransportRoles\Replay

GFI MailEssentials installato in Microsoft® Exchange Server 2003

Spostare i messaggi (in formato .txt) dalla cartella **failedmails** alla seguente:

<percorso di installazione di Microsoft Exchange>\Exchsrvr\Mailroot\vsi 1\PickUp

GFI MailEssentials installato sul server gateway.

Spostare i messaggi (in formato .txt) dalla cartella **failedmails** alla seguente:

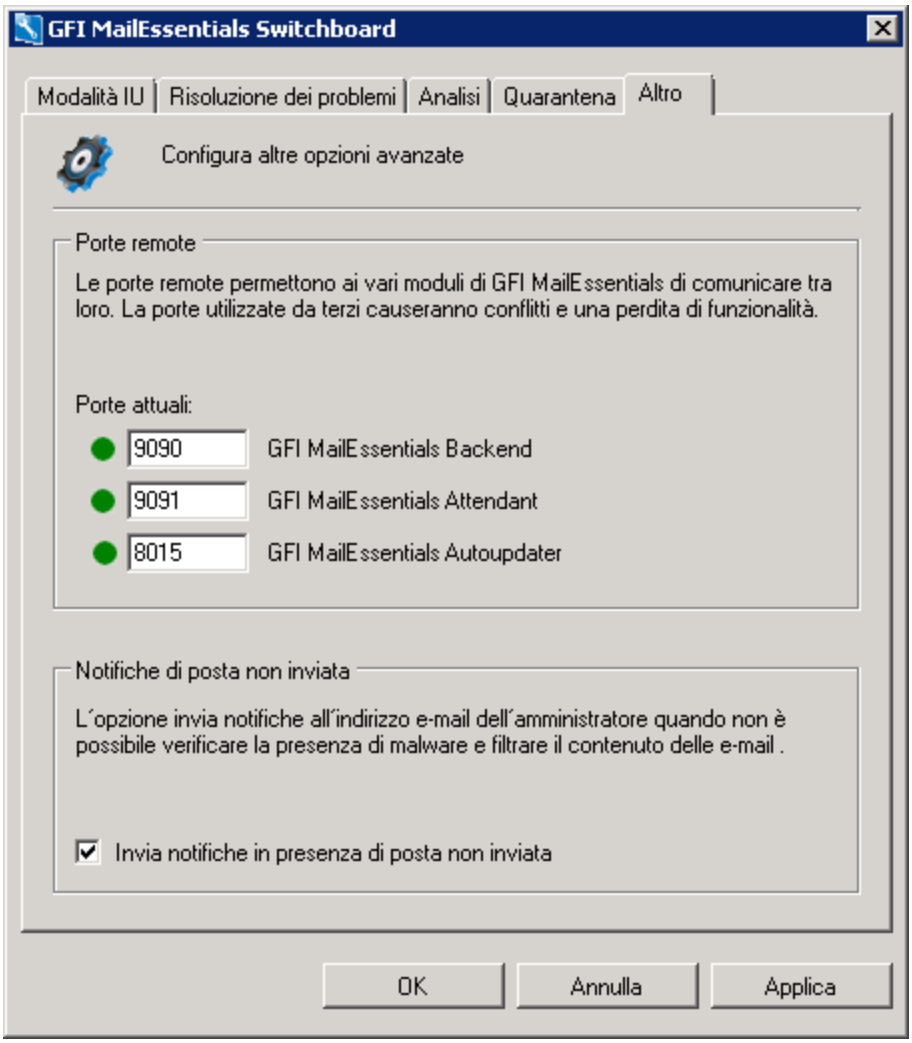
<unità>\Inetpub\mailroot\Pickup

11.4.2 Notifiche messaggi di posta elettronica non riusciti

GFI MailEssentials può essere configurato per notificare all'amministratore quando un messaggio non viene elaborato.

L’indirizzo di posta elettronica dell’amministratore può essere configurato nel nodo Impostazioni generali di GFI MailEssentials. Per ulteriori informazioni, fare riferimento a Indirizzo e-mail amministratore (pagina 241).

1. Avviare GFI MailEssentials Switchboard da **Start > Tutti i programmi > GFI MailEssentials > Switchboard** e selezionare la scheda **Altro**.


GFI MailEssentials Switchboard
Modalità IU
Risoluzione dei problemi
Analisi
Quarantena
Altro
Configura altre opzioni avanzate
Porte remote
Le porte remote permettono ai vari moduli di GFI MailEssentials di comunicare tra loro. La porte utilizzate da terzi causeranno conflitti e una perdita di funzionalità.
Porte attuali:
9090
GFI MailEssentials Backend
9091
GFI MailEssentials Attendant
8015
GFI MailEssentials Autoupdater
Notifiche di posta non inviata
L´opzione invia notifiche all´indirizzo e-mail dell´amministratore quando non è possibile verificare la presenza di malware e filtrare il contenuto delle e-mail .
Invia notifiche in presenza di posta non inviata
OK
Annulla
Applica

Schermata 138: abilitazione notifica messaggi di posta elettronica non riusciti

2. Selezionare **Invia notifiche in presenza di posta non inviata**.

3. Fare clic su **Applica**.

> **NOTA**
> Durante l’esecuzione di questa operazione, alcuni servizi vengono arrestati temporaneamente. Questo potrebbe incidere sul flusso della posta e/o la scansione della posta.

4. Per eseguire il riavvio dei servizi visualizzati, fare clic su **Sì**.

5. Fare clic su **OK**.

11.5 Analisi

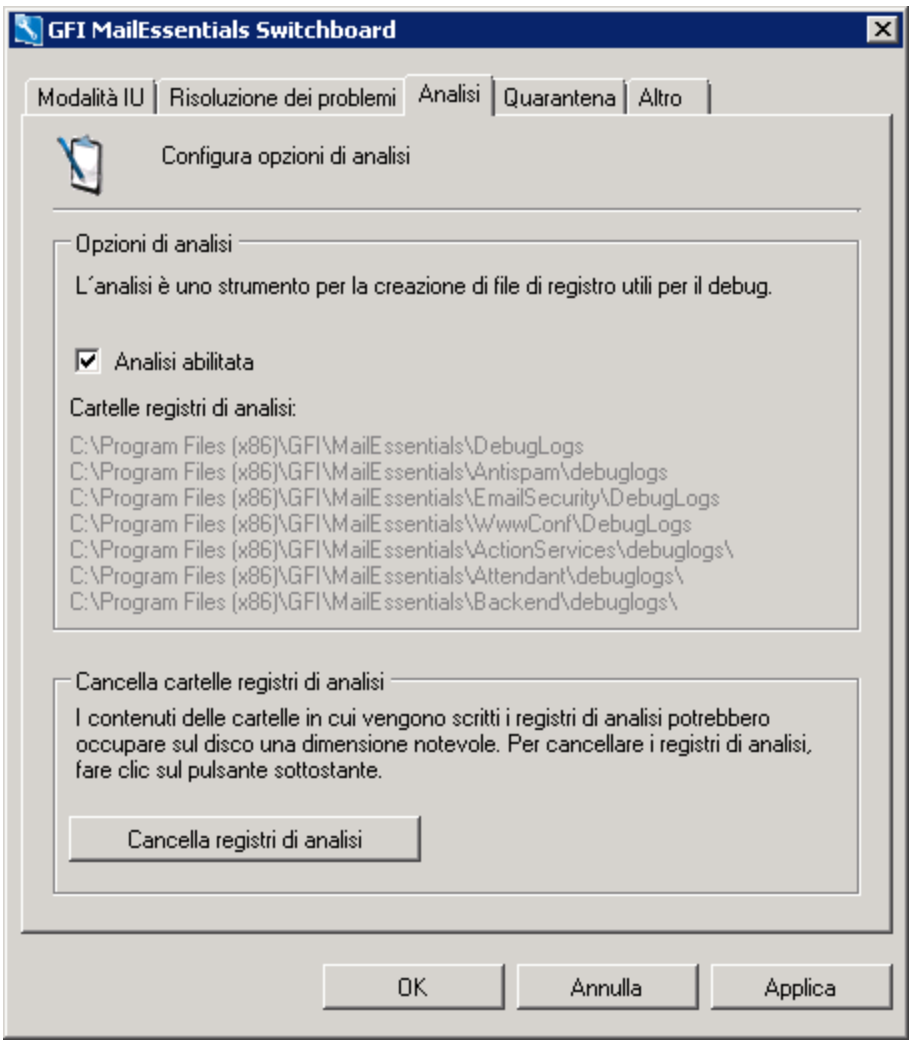
GFI MailEssentials consente di creare file di registro per il debugging. Utilizzare la traccia per la risoluzione dei problemi oppure per contattare il supporto di GFI. Disabilitare la traccia se vi sono problemi di prestazioni con il computer di GFI MailEssentials.

Quando abilitato, GFI MailEssentials archivia una serie di file di registro nelle seguenti cartelle:

- <*GFI MailEssentials percorso di installazione*>*GFI**MailEssentials*\DebugLogs\
- <*GFI MailEssentials percorso di installazione*>*GFI**MailEssentials*\Antispam\DebugLogs\
- <*GFI MailEssentials percorso di installazione*>*GFI**MailEssentials*\EmailSecurity\DebugLogs\
- <*GFI MailEssentials percorso di installazione*>*GFI**MailEssentials*\WwwConf\DebugLogs\
- <*GFI MailEssentials percorso di installazione*>*GFI**MailEssentials*\ActionServices\DebugLogs\
- <*GFI MailEssentials percorso di installazione*>*GFI**MailEssentials*\Attendant\DebugLogs\
- <*GFI MailEssentials percorso di installazione*>*GFI**MailEssentials*\Backend\DebugLogs\

Per abilitare o disabilitare la traccia:

1. Avviare GFI MailEssentials Switchboard da **Start > Tutti i programmi > GFI MailEssentials > Switchboard** e selezionare la scheda **Traccia**.


GFI MailEssentials Switchboard
Modalità IU
Risoluzione dei problemi
Analisi
Quarantena
Altro
Configura opzioni di analisi
Opzioni di analisi
L´analisi è uno strumento per la creazione di file di registro utili per il debug.
Analisi abilitata
Cartelle registri di analisi:
C:\Program Files (x86)\GFI\MailEssentials\DebugLogs
C:\Program Files (x86)\GFI\MailEssentials\Antispam\debuglogs
C:\Program Files (x86)\GFI\MailEssentials\EmailSecurity\DebugLogs
C:\Program Files (x86)\GFI\MailEssentials\WwwConf\DebugLogs
C:\Program Files (x86)\GFI\MailEssentials\ActionServices\debuglogs\
C:\Program Files (x86)\GFI\MailEssentials\Attendant\debuglogs\
C:\Program Files (x86)\GFI\MailEssentials\Backend\debuglogs\
Cancella cartelle registri di analisi
I contenuti delle cartelle in cui vengono scritti i registri di analisi potrebbero occupare sul disco una dimensione notevole. Per cancellare i registri di analisi, fare clic sul pulsante sottostante.
Cancella registri di analisi
OK
Annulla
Applica

Schermata 139: configura opzioni di traccia

2. Per abilitare o disabilitare la traccia, selezionare o disabilitare rispettivamente **Analisi abilitata**.

> **NOTA**
> Durante l'esecuzione di questa operazione, alcuni servizi vengono arrestati temporaneamente. Questo potrebbe incidere sul flusso della posta e/o la scansione della posta.

3. Per eseguire il riavvio dei servizi visualizzati, fare clic su **Sì**.

4. Fare clic su **OK**.

Cancella registri di analisi

Per eliminare tutti i file di traccia:

1. Avviare GFI MailEssentials Switchboard da **Start > Tutti i programmi > GFI MailEssentials > Switchboard** e selezionare la scheda **Traccia**.

> **NOTA**
> Durante l'esecuzione di questa operazione, alcuni servizi vengono arrestati temporaneamente. Questo potrebbe incidere sul flusso della posta e/o la scansione della posta.

2. Fare clic su **Cancella registri di analisi** e fare clic su **Sì**per riavviare i servizi visualizzati.

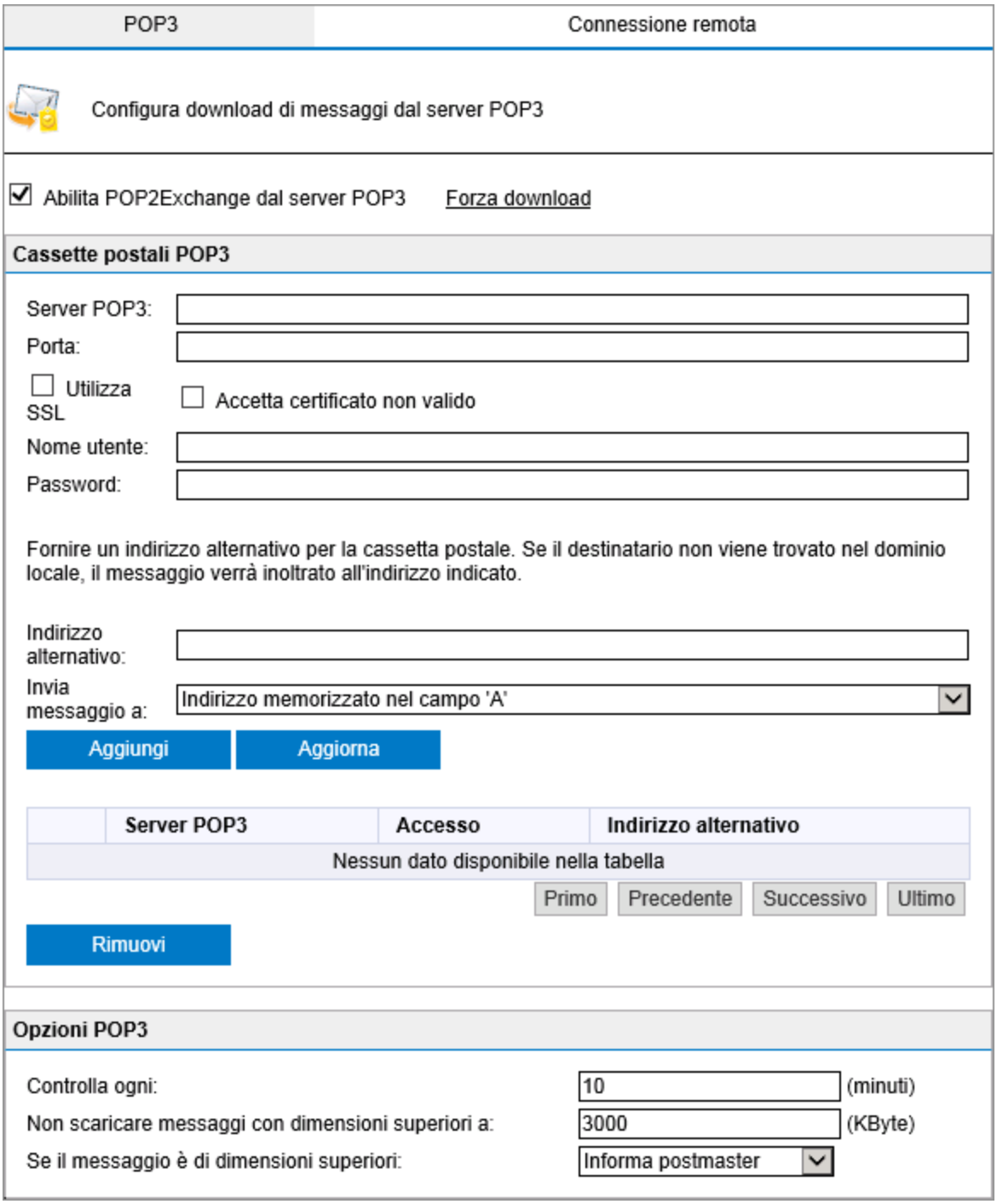
3. Al termine, fare clic su **OK**.

11.6 POP2Exchange - Download messaggi dal server POP3

POP2Exchange scarica i messaggi da un server POP3, li elabora e quindi li invia al server di posta locale. Nel caso di GFI MailEssentials, evitare possibilmente l'utilizzo di POP3 e ricorrere a SMTP, dato che POP3 è studiato per i client di posta elettronica e non per i server di posta. A prescindere da questo, e per risolvere le situazioni dove non è disponibile l'indirizzo IP statico richiesto da SMTP, GFI MailEssentials può ricorrere a POP3 per il recupero della posta.

11.6.1 Configurazione downloader POP3

1. Andare al nodo **POP2Exchange**.



Schermata 140: downloader POP3 di GFI MailEssentials

2. Dalla scheda **POP3**, per abilitare il downloader POP3, selezionare **Abilita POP2Exchange dal server POP3**.

3. Nella casella **Cassette postali POP3**, specificare i dettagli dei server POP3 da cui scaricare i messaggi:

Opzione	Descrizione
Server POP3	Immettere l'indirizzo IP del server POP3 da cui scaricare i messaggi.

Opzione	Descrizione
Porta	Digitare la porta POP3. Per impostazione predefinita, POP3 utilizza la porta 110 o 995 in presenza di una connessione sicura.
Utilizza SSL	Selezionare se il server POP3 richiede una connessione protetta.
Accetta certificato non valido	Scegliere questa opzione per ignorare i certificati non verificati dal server POP3. Si consiglia di deselezionare questa opzione e accertarsi che tutti i certificati siano convalidati.
Accesso e password	Specificare le credenziali per eseguire l'accesso alla cassetta postale POP3.
Indirizzo alternativo	Se i messaggi nella cassetta postale sono indirizzati a un destinatario che non è in uno dei domini locali di GFI MailEssentials, i messaggi verranno inoltrati a quell'indirizzo. Accertarsi che sia un indirizzo locale, configurato sul server di posta e protetto da GFI MailEssentials.
Invia messaggio a:	Scegliere: » **Indirizzo memorizzato nel campo 'A'**: GFI MailEssentials analizzerà l'intestazione del messaggio, inoltrando di conseguenza l'e-mail. Se l'analisi del messaggio non riesce, questo viene inviato all'indirizzo di posta elettronica indicato nel campo **Indirizzo alternativo**. » **Indirizzo alternativo**: GFI MailEssentials non analizza le intestazioni delle e-mail e tutte le e-mail di questa cassetta postale vengono inoltrate all'indirizzo e-mail configurato in **Indirizzo alternativo**.

4. Fare clic su **Aggiungi** per aggiungere i dati del server POP3. Scegliere un server POP3 aggiuntivo e fare clic su **Aggiorna** per sostituirlo con le impostazioni appena inserite.

5. Per aggiungere più server POP3, ripetere i passaggi di cui sopra.

6. In **Opzioni POP3**, configurare:

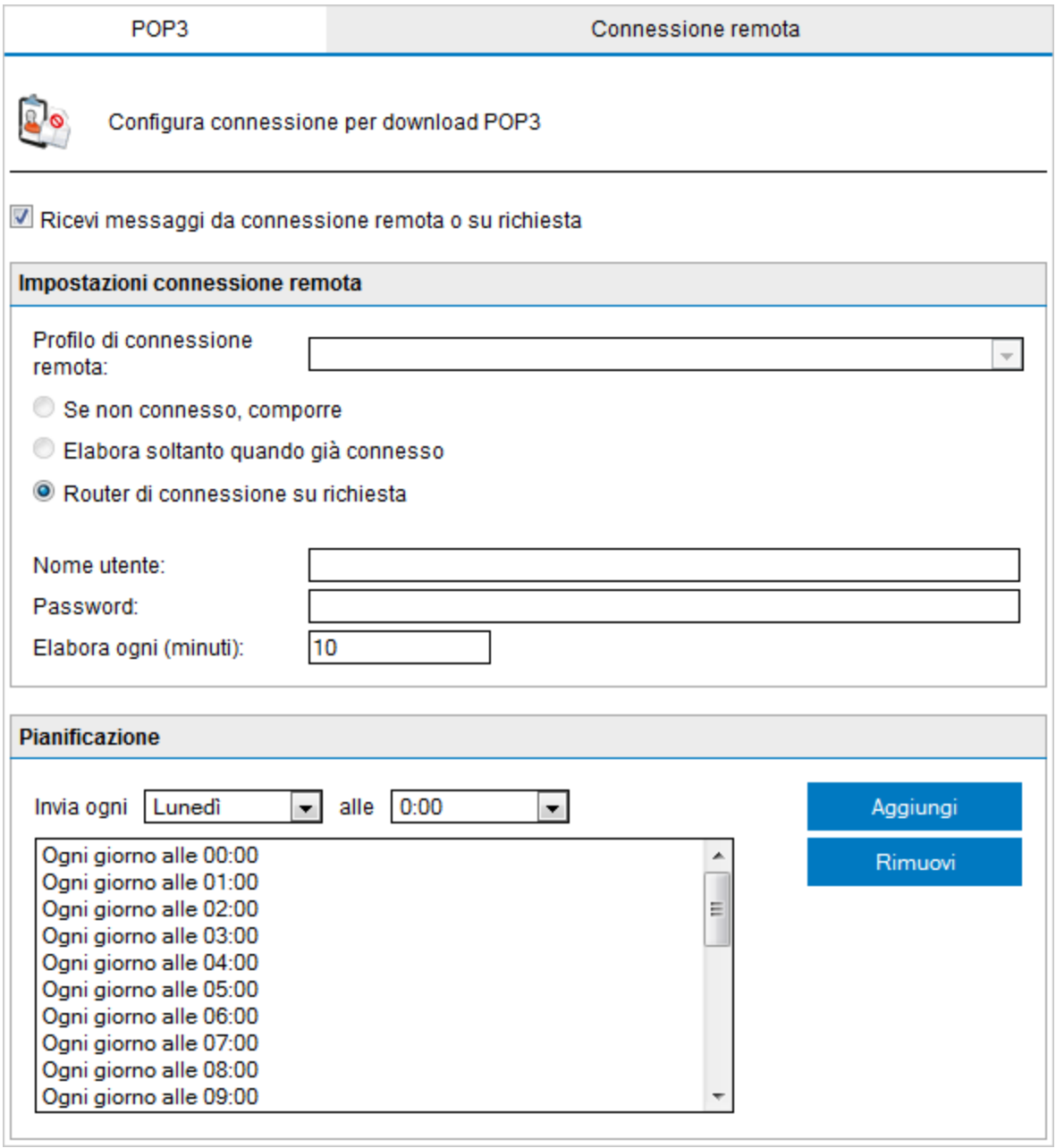
Opzione	Descrizione
Controlla ogni (minuti)	Indicare l'intervallo di download in minuti.
Non scaricare messaggi con dimensioni superiori a	Indicare una dimensione massima di download in KByte. Se i messaggi la superano, non verranno scaricati.
Se il messaggio è di dimensioni superiori:	Scegliere di eliminare i messaggi superiori alle dimensioni massime consentite, oppure di inviare un messaggio al postmaster.

8. Fare clic su **Applica**.

11.6.2 Configurazione opzioni di connessione remota

1. Andare al nodo **POP2Exchange** e selezionare la scheda **Connessione remota**.

2. Selezionare **Ricevi messaggi da connessione remota o su richiesta**.



Schermata 141: Opzioni di connessione remota

3. Selezionare un profilo di connessione remota e configurare un nome di accesso e password. Sono disponibili le seguenti opzioni:

Opzione	Descrizione
Utilizza profilo di networking di connessione remota	Scegliere il profilo di networking di connessione remota da utilizzare.
Se non connesso, comporre	GFI MailEssentials eseguirà la connessione remota solo in assenza di connessione.
Elabora soltanto quando già connesso	GFI MailEssentials elaborerà la posta solo in presenza di una connessione già esistente.

Opzione	Descrizione
Router di connessione su richiesta:	Nel caso la connessione a Internet sia stabilita automaticamente (come con un router di connessione su richiesta), selezionare questa opzione. GFI MailEssentials sceglierà la posta all'intervallo indicato senza attivare una connessione remota.
Nome utente e password	Immettere le credenziali usate per accedere al proprio ISP.
Elabora ogni (minuti)	Inserire l'intervallo in minuti.

4. Nell'area **Pianificazione**, indicare le ore in cui GFI MailEssentials deve eseguire la connessione remota per prelevare la posta.

5. Fare clic su **Applica**.

11.7 Spostamento messaggi spam nelle cartelle della cassetta postale degli utenti

Quando GFI MailEssentials è installato su Microsoft® Exchange Server, i messaggi spam possono essere salvati in una cartella della cassetta postale degli utenti. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148).

Se GFI MailEssentials **NON** è installato su Microsoft® Exchange Server, i messaggi spam non possono essere inoltrati a una cartella della cassetta postale specifica dell'utente mediante le Operazioni spam. Tuttavia, i messaggi possono essere ancora inoltrati alla cassetta postale dell'utente, come di seguito illustrato.

11.7.1 Microsoft® Exchange 2007/2010

Per configurare Microsoft® Exchange 2007/2010 per l'inoltro dei messaggi contrassegnati nella cartella della cassetta postale Posta indesiderata dell'utente, è necessario creare una regola di trasporto.

IMPORTANTE
Da Operazioni spam GFI MailEssentials, selezionare solo l'opzione Contrassegna il messaggio con un testo specifico. Se si sceglie un'altra azione, i messaggi rilevati come spam non raggiungeranno la cassetta postale dell'utente, pertanto le regole di trasporto configurate non saranno applicabili.

Per creare una regola di trasporto in Exchange 2007/2010:

1. Avviare Microsoft® Exchange Management Console.

2. Espandere il nodo **Microsoft Exchange > Configurazione dell'organizzazione > Trasporto hub** e scegliere il nodo **Regole di trasporto**.

3. Fare clic su **Nuova regola di trasporto**.

4. Digitare un nome per la nuova regola (ad esempio, GFI MailEssentials `SPAM`), quindi fare clic su **Avanti**.

5. Nell'area **Condizioni**, selezionare **Quando il campo Oggetto contiene parole specifiche**.

6. Nell'area **Modifica regola**, fare clic su **Parole specifiche** per inserire le parole utilizzate per il contrassegno. Digitare il contrassegno specificato nelle operazioni spam di ciascun filtro antispam (ad esempio, `[SPAM]`) quindi fare clic su **Aggiungi**. Una volta aggiunte tutte le parole, fare clic su **OK** e quindi su **Avanti**.

7. Nell'area **Azioni**, selezionare **Imposta il livello di probabilità di posta indesiderata su valore**.

8. Nell'area **Modifica regola**, fare clic su **0** e impostare il livello di probabilità su **9**. Selezionare **OK** e fare clic su **Avanti**.

9. (Facoltativo) Impostare eventuali eccezioni alla regola di trasporto, quindi fare clic su **Avanti**.

10. Per creare la nuova regola di trasporto, fare clic su **Nuova**.

> **NOTA**
> Assicurarsi che la cartella Posta indesiderata sia abilitata per le cassette postali degli utenti.

Adesso la regola di trasporto creata inoltrerà nella cartella Posta indesiderata degli utenti tutti i messaggi con il contrassegno GFI MailEssentials.

11.7.2 Microsoft® Exchange Server 2003

GFI MailEssentials comprende un'utilità di Gestione regole che sposta automaticamente nella cassetta postale degli utenti i messaggi contrassegnati come spam.

> **IMPORTANTE**
> Per utilizzare Gestione regole, da Operazioni spam, selezionare l'opzione **Contrassegna il messaggio con un testo specifico**, quindi indicare il tag.

Installazione di Gestione regole su Microsoft® Exchange Server

1. Dal computer dove è installato GFI MailEssentials aprire il percorso:

<*GFI MailEssentials percorso di installazione*>\GFI\MailEssentials\Antispam\

2. Copiare i seguenti file in una cartella di Microsoft® Exchange Server:

- rulemgmtres.dll
- rulemgmt.exe
- rule.dll
- gfi_log.dll

3. Da Microsoft® Exchange Server, aprire il prompt dei comandi e impostare come directory il percorso dove sono stati copiati i file di Gestione regole.

4. Dal prompt dei comandi, digitare: `regsvr32 rule.dll`

5. Dopo la conferma, fare clic su **OK**.

Avvio di Gestione regole

1. Da Microsoft® Exchange Server, aprire il percorso dove sono stati copiati i file di Gestione regole, quindi aprire **rulemgmt.exe**.

2. Selezionare un profilo di Microsoft® Outlook (profilo MAPI) oppure crearne uno nuovo per l'accesso. L'operazione dovrà essere eseguita solo al primo utilizzo di Gestione regole.

3. Fare clic su **OK** per avviare Gestione regole.

4. La finestra principale di Gestione regole visualizza tutte le cassette postali abilitate su Microsoft® Exchange Server. Il colore delle cassette postali indica lo stato della cassetta:

» Blu: la cassetta postale ha le regole configurate.

» Nero: la cassetta postale non ha regole configurate.

Impostazione nuove regole

1. Selezionare le cassette postali per cui impostare una regola e fare clic su **Configura**….

> **NOTE**
> 1. Le nuove regole possono essere aggiunte alle cassette postali che già ne contengono.
> 2. Per configurare la medesima regola applicabile a tutte le cassette postali, selezionare cassette postali multiple.

2. Nella casella di testo **Condizione regola**, immettere il contrassegno assegnato al messaggio spam nelle operazioni spam di GFI MailEssentials.

3. Indicare **Azione regola**:

» Per eliminare un messaggio con un oggetto che contiene la condizione della regola, selezionare **Elimina**.

» Per spostare il messaggio spam in una cartella della cassetta postale, selezionare **Sposta a:**. Digitare il percorso della cartella dove salvare i messaggi spam. Se si indica Posta in arrivo\Spam, verrà creata una cartella spam nella cartella Posta in arrivo. Se si specifica solo Spam, allora la cartella verrà creata al livello superiore (lo stesso della Posta in arrivo).

4. Per salvare le regole impostate, fare clic su **Applica**.

Gestione di regole multiple

Nella stessa cassetta postale è possibile impostare più di una regola.

Esempio: Eliminare i messaggi contrassegnati con `[Phishing]` e spostare i messaggi contrassegnati con `[SPAM]` nella cartella Posta in arrivo\Spam.

1. Per avviare la finestra di dialogo Regole, fare doppio clic su una cassetta postale.

2. Viene visualizzato un elenco delle regole applicabili alla cassetta postale selezionata.

» Per aggiungere una nuova regola, fare clic su **Aggiungi regola**.

» Selezionare una regola, quindi fare clic su **Modifica regola** per cambiare le impostazioni della regola selezionata.

» Selezionare una regola, quindi fare clic su **Cancella regola** per eliminare la regola selezionata.

3. Fare clic su **Applica** per salvare le impostazioni.

11.8 Spostamento spam nella cartella di Exchange 2010

Quando GFI MailEssentials è installato su Microsoft® Exchange 2010 server, è necessario creare un utente dedicato per l'utilizzo dell'operazione antispam **-Consegnare messaggio di posta elettronica alla cassetta postale - Nella cartella secondaria della cassetta postale di Exchange**. Configurare l'utente dedicato da GFI MailEssentials Switchboard.

> **NOTA**
> Se l'utente non è configurato, lo spam non potrà essere spostato in una cartella secondaria della cassetta postale.

Per configurare un utente dedicato:

1. Avviare GFI MailEssentials Switchboard da **Start > Tutti i programmi > GFI MailEssentials > Switchboard**.

2. Selezionare la scheda **Sposta in Exchange**.

> **NOTA**
> Questa scheda viene visualizzata solo quando GFI MailEssentials è installato su Microsoft® Exchange 2010 server.

3. Per indicare l'utente dedicato, fare clic su **Specifica account utente...**.

4. Selezionare una delle seguenti opzioni:

Opzione	Descrizione
Sposta spam utilizzando un utente creato automaticamente	Permettere a GFI MailEssentials di creare automaticamente un utente con tutti i diritti necessari.
Sposta spam utilizzando il seguente account utente	Utilizzare un utente creato manualmente. Specificare le credenziali **Dominio\nomeutente** e **Password**) di un utente dedicato e fare clic su **Imposta diritti di accesso** per assegnare i diritti necessari all'utente specificato.

> **NOTA**
> Le credenziali dell'utente specificate manualmente devono essere dedicate esclusivamente a questa funzione. Nome utente, password e altre proprietà non devono essere modificate da Microsoft® Exchange o Active Directory, altrimenti questa funzione non sarà valida.

5. Per applicare le impostazioni, fare clic su **Fine**.

6. Fare clic su **OK**.

11.9 Sincronizzazione dati di configurazione

Se GFI MailEssentials è installato su più server, è importante che i dati di configurazione restino sincronizzati tra i server.

GFI MailEssentials consente questa procedura attraverso due funzionalità che mantengono aggiornate le installazioni multiple di GFI MailEssentials:

» Agente di sincronizzazione antispam: questo servizio automatizza la procedura di mantenere sincronizzate le impostazioni antispam tra installazioni separate attraverso l'uso del servizio Microsoft® BITS.

» Strumento di esportazione/importazione di configurazione : questa applicazione consente l'esportazione manuale delle impostazioni di configurazione di GFI MailEssentials e la successiva importazione in altre installazioni.

11.9.1 Agente di sincronizzazione antispam

Funzionamento

L'agente di sincronizzazione antispam opera nel seguente modo:

1. Un computer server che ospita GFI MailEssentials viene configurato come server master.

2. Gli altri computer server dove è installato GFI MailEssentials vengono configurati come server slave.

3. Utilizzando il servizio Microsoft® BITS, i server slave caricano un file di archivio (contenente le impostazioni) in una cartella virtuale IIS ospitata sul server master.

4. Quando il server master raccoglie tutti i dati dei server slave, tali dati vengono estratti dagli archivi singoli e uniti in un file di archivio centrale.

5. I server slave scaricano questo file di archivio centrale e si occupano di estrarlo e aggiornare l'installazione locale di GFI MailEssentials, così da sfruttare al meglio le nuove impostazioni.

> **NOTE**
>
> 1. In tutti i server che collaborano alla sincronizzazione delle impostazioni antispam deve essere installata la stessa versione di GFI MailEssentials.
>
> 2. I file caricati e scaricati dall'agente di sincronizzazione vengono compressi per limitare il traffico sulla rete.
>
> 3. Quando la sincronizzazione ha esito negativo per 3 volte consecutive, GFI MailEssentials notifica l'amministratore via posta elettronica.
>
> 4. Le impostazioni dei motori di sicurezza della posta e del filtro dei contenuti non sono sincronizzate dall'agente.

Passaggio 1: configurazione della directory virtuale dell'agente di sincronizzazione sul server master

Note importanti

1. È possibile configurare solo un server master per volta.

2. Una directory virtuale IIS deve essere creata solo sul server master.

3. Per configurare un server come server master, deve soddisfare le seguenti configurazioni di sistema:

Sistema operativo	IIS	Servizio trasferimento intelligente in background (BITS)
Microsoft® Windows Server 2012	Obbligatorio	Obbligatorio Abilitare il servizio BITS dall'**Aggiunta guidata ruoli e funzionalità** di Server Manager.
Microsoft®Windows Server 2008 con SP1 o versioni successive	Obbligatorio	Obbligatorio Per ulteriori informazioni sulle modalità d'installazione di BITS, fare riferimento a http://go.gfi.com/?pageid=ME_InstallBITS2008
Microsoft®Windows Server 2003 con SP1 o versioni successive	Obbligatorio	Obbligatorio Per ulteriori informazioni sulle modalità d'installazione di BITS, fare riferimento a http://go.gfi.com/?pageid=ME_InstallBITS2003

Configurazione directory virtuale

In Gestione Internet Information Services (IIS), configurare una directory virtuale condivisa sul sito Web predefinito del server master, come descritto di seguito.

IIS 7.0

a. Caricare la console **Gestione Internet Information Services (IIS)**, fare clic con il pulsante destro del mouse sul sito Web predefinito e selezionare **Aggiungi directory virtuale**.

b. Nella finestra di dialogo **Aggiungi directory virtuale**, digitare `MESynchAgent` come alias per la directory virtuale.

c. Specificare un percorso dove archiviare i contenuti della directory virtuale, quindi fare clic su **OK** per aggiungerla.

> **NOTA**
> prendere nota del percorso configurato come riferimento.

d. Selezionare la directory virtuale **MESynchAgent** e da Visualizzazione funzionalità, fare doppio clic su **Impostazioni SSL**.

e. Disabilitare la casella di controllo **Richiedi SSL** e fare clic su **Applica**.

f. Tornare alla Visualizzazione funzionalità della directory virtuale appena aggiunta, quindi fare doppio clic su **Autenticazione**.

g. Assicurarsi che sia abilitato solo **Autenticazione di base**, mentre le altre opzioni sono disabilitate.

h. Fare clic con il pulsante destro del mouse su **Autenticazione di base** e selezionare **Modifica…** per specificare **Dominio predefinito** e **Area autenticazione** del nome utente e password utilizzati per l'autenticazione da parte dei computer slave. Fare clic su **OK** e **Applica**.

i. Tornare alla Visualizzazione funzionalità della directory virtuale **MESynchAgent**, quindi fare doppio clic su **Processi di caricamento BITS**.

j. Selezionare **Consenti ai clienti di caricare file** e seleziona **Usa impostazioni predefinite del sito padre**. Fare clic su **Applica**.

IIS 6.0

a. Dalla console **Gestione Internet Information Services (IIS)**, fare clic con il pulsante destro del mouse sul sito Web predefinito e selezionare **Nuovo > Directory virtuale**.

b. In **Creazione guidata Directory virtuale**, specificare `MESynchAgent` come alias per la directory virtuale e fare clic su **Avanti**.

c. Specificare un percorso dove archiviare i contenuti della directory virtuale, quindi fare clic su **Avanti**.

> **NOTA**
> prendere nota del percorso configurato come riferimento.

d. Selezionare le caselle di controllo **Lettura** e **Scrittura** e deselezionare tutte le altre. Fare clic su **Avanti** e infine su **Fine**.

e. Fare clic con il pulsante destro del mouse sulla nuova directory virtuale **MESynchAgent** e selezionare **Proprietà**.

f. Selezionare la scheda **Protezione directory** e nel gruppo **Controllo autenticazione e accesso** fare clic su **Modifica**.

g. Nel gruppo **Accesso con autenticazione**, selezionare **Autenticazione di base** e specificare **Dominio predefinito** e **Area autenticazione** del nome utente e della password utilizzati per l'autenticazione da parte dei computer slave.

> **NOTA**
> Assicurarsi che tutte le altre caselle di controllo siano deselezionate.

h. Fare clic su **OK**.

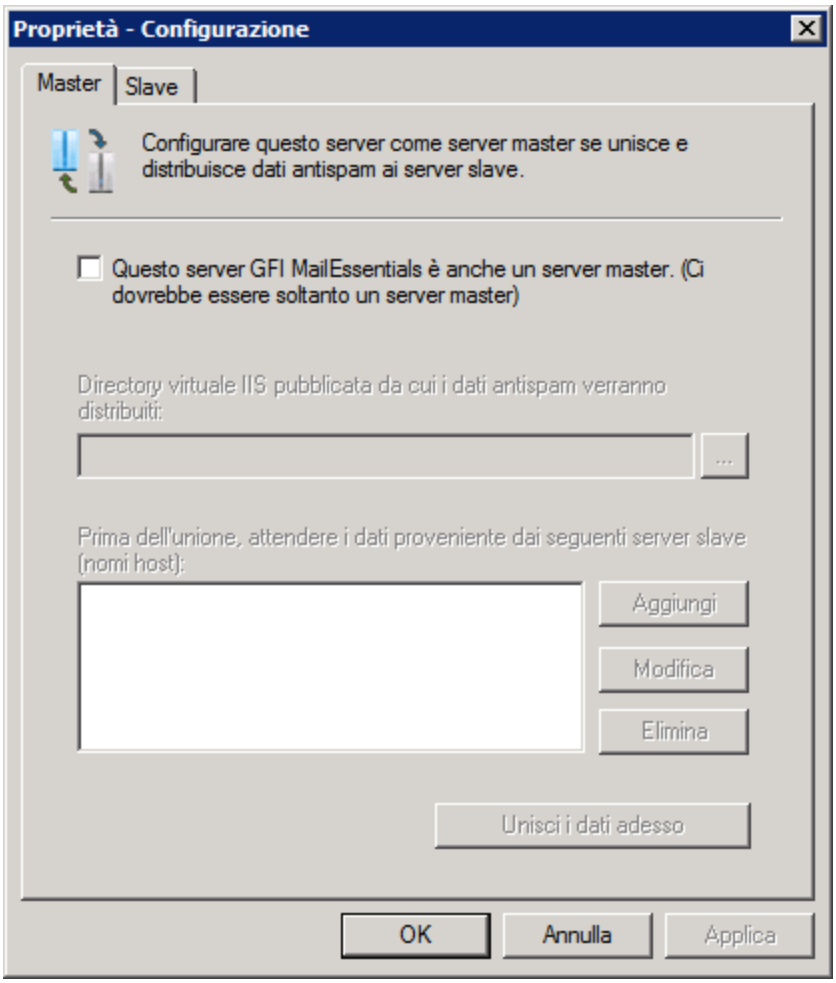
i. Selezionare la scheda **Estensione server BITS** e selezionare **Consenti il trasferimento di dati in questa directory virtuale**.

j. Fare clic su **OK** per chiudere le proprietà della finestra di dialogo della directory virtuale.

Passaggio 2: configurazione del server master di GFI MailEssentials

1. Dal server master, selezionare <*GFI MailEssentials percorso di installazione*>\GFI\MailEssentials\`AntiSpam\` quindi aprire **mesentcfg.msc**.

2. Fare clic con il pulsante destro su **Agente di sincronizzazione antispam > Configurazione** quindi selezionare **Proprietà**.


Proprietà - Configurazione
Master
Slave
Configurare questo server come server master se unisce e distribuisce dati antispam ai server slave.
Questo server GFI MailEssentials è anche un server master. (Ci dovrebbe essere soltanto un server master)
Directory virtuale IIS pubblicata da cui i dati antispam verranno distribuiti:
...
Prima dell'unione, attendere i dati proveniente dai seguenti server slave (nomi host):
Aggiungi
Modifica
Elimina
Unisci i dati adesso
OK
Annulla
Applica

Schermata 142: configurazione di un server master

3. Dalla scheda **Master**, selezionare **Questo server GFI MailEssentials Configuration è anche un server master** e digitare il percorso completo della cartella configurata per contenere i contenuti della directory virtuale **MESynchAgent**.

4. Selezionare il pulsante **Aggiungi** e immettere il nome host del server slave. Fare clic su **OK** per aggiungerlo all'elenco. Ripetere il passaggio e aggiungere tutti gli altri server slave.

> **NOTA**
> Assicurarsi di configurare come server slave tutti i computer dell'elenco, altrimenti l'agente di sincronizzazione del server master non unirà i dati.

> **NOTA**
> Un server master può fungere anche da server slave al tempo stesso. In questo caso, il server unirà i propri dati a quelli caricati dagli altri server slave. Affinché questo funzioni, è necessario aggiungere il nome host del server master all'elenco di server slave.

5. Se necessario, scegliere un server slave dall'elenco e fare clic su **Modifica** o **Elimina** per modificarlo o eliminarlo.

6. Fare clic su **OK**.

Passaggio 3: configurazione server slave

Note importanti

1. Per configurare un server come server slave, deve soddisfare le seguenti specifiche di sistema:

» Microsoft® Windows Server 2008

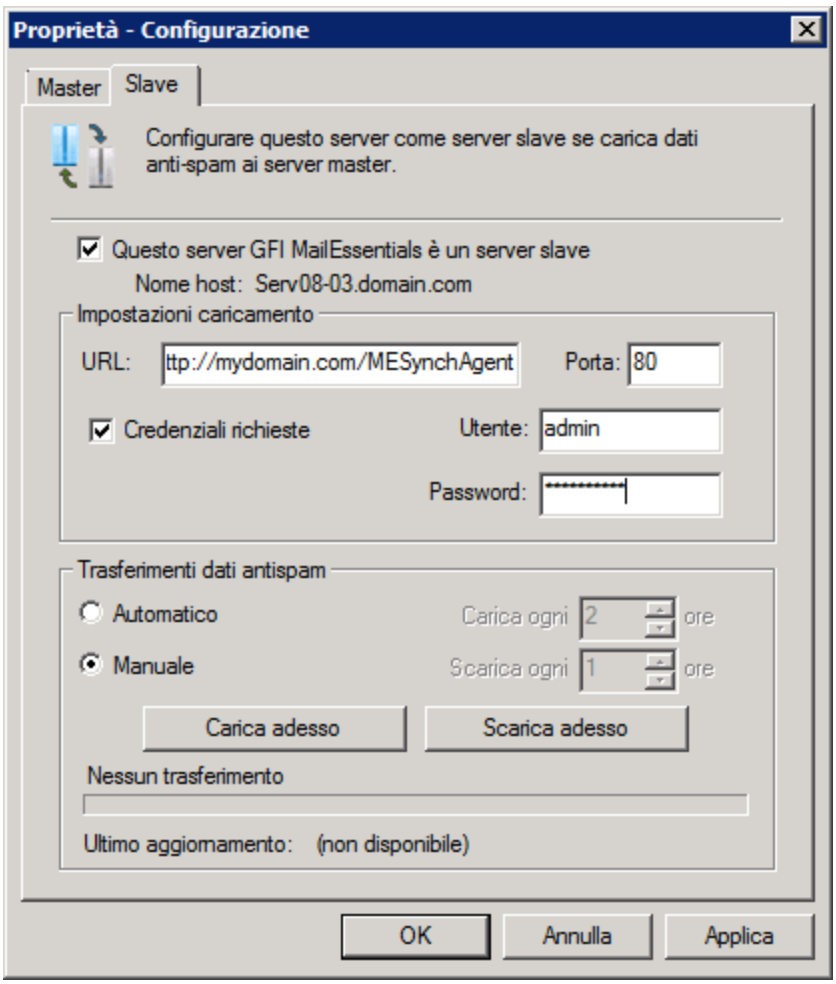
» Microsoft® Windows Server 2003: si consiglia di scaricare l'aggiornamento del client BITS 2.0 da: http://go.gfi.com/?pageid=ME_BITS2003Update

2. I server slave caricano automaticamente un file di archivio, contenente le impostazioni antispam della directory virtuale IIS sul server master, così sui server slave non deve essere creata nessuna directory virtuale.

Configurazione server slave

1. Dal server slave, selezionare `<GFI MailEssentials percorso di installazione>\GFI\MailEssentials\AntiSpam\` quindi aprire **mesentcfg.msc**.

2. Fare clic con il pulsante destro sul nodo **Agente di sincronizzazione antispam > Configurazione** quindi selezionare **Proprietà**.



Schermata 143: configurazione server slave

3. Dalla scheda **Slave**, selezionare **Questo server GFI MailEssentials è un server slave.**

4. Nel campo URL, specificare nel seguente formato l'URL completo della directory virtuale ospitata sul server master:

`http://<nome dominio server master>/MESynchAgent`

» Esempio: `http://mydomain.com/MESynchAgent`

5. Nel campo **Porta**, indicare la porta utilizzata dal server master per accettare le comunicazioni HTTP.

> **NOTA**
> Per impostazione predefinita, il valore predefinito della porta è impostato su **80**, che è la porta standard utilizzata per HTTP.

6. Selezionare **Credenziali richieste** e digitare le credenziali utilizzate per eseguire l'autenticazione con il server master.

7. Selezionare:

Opzione	Descrizione
Automatico	La sincronizzazione avviene automaticamente a intervalli impostati. Nel campo **Carica ogni**, indicare l'intervallo di caricamento in ore che determina la frequenza con cui il server slave caricherà le proprie impostazioni sul server master. Nel campo **Scarica ogni**, indicare l'intervallo di scaricamento in ore che determina la frequenza con cui il server slave controllerà la presenza di aggiornamenti sul server master e ne eseguirà il download. Note importanti sulla configurazione dell'intervallo: » L'intervallo orario per il caricamento e il download non può avere il medesimo valore. » L'intervallo orario può essere impostato su qualsiasi valore compreso tra 1 e 240 ore. » È consigliabile configurare l'intervallo di download con un valore inferiore a quello di caricamento. » Si consiglia anche di utilizzare il medesimo intervallo per tutti i server slave. Esempio: Impostare l'intervallo di download a 3 ore e quello di caricamento a 4 ore. In tal modo, i download saranno più frequenti dei caricamenti.
Manuale	Caricare e scaricare manualmente il file di archivio. Per caricare le impostazioni del server slave sul server master, fare clic su **Carica adesso**. Per scaricare le impostazioni unite aggiornate dal server master, fare clic su **Scarica adesso**.

8. Fare clic su **OK**.

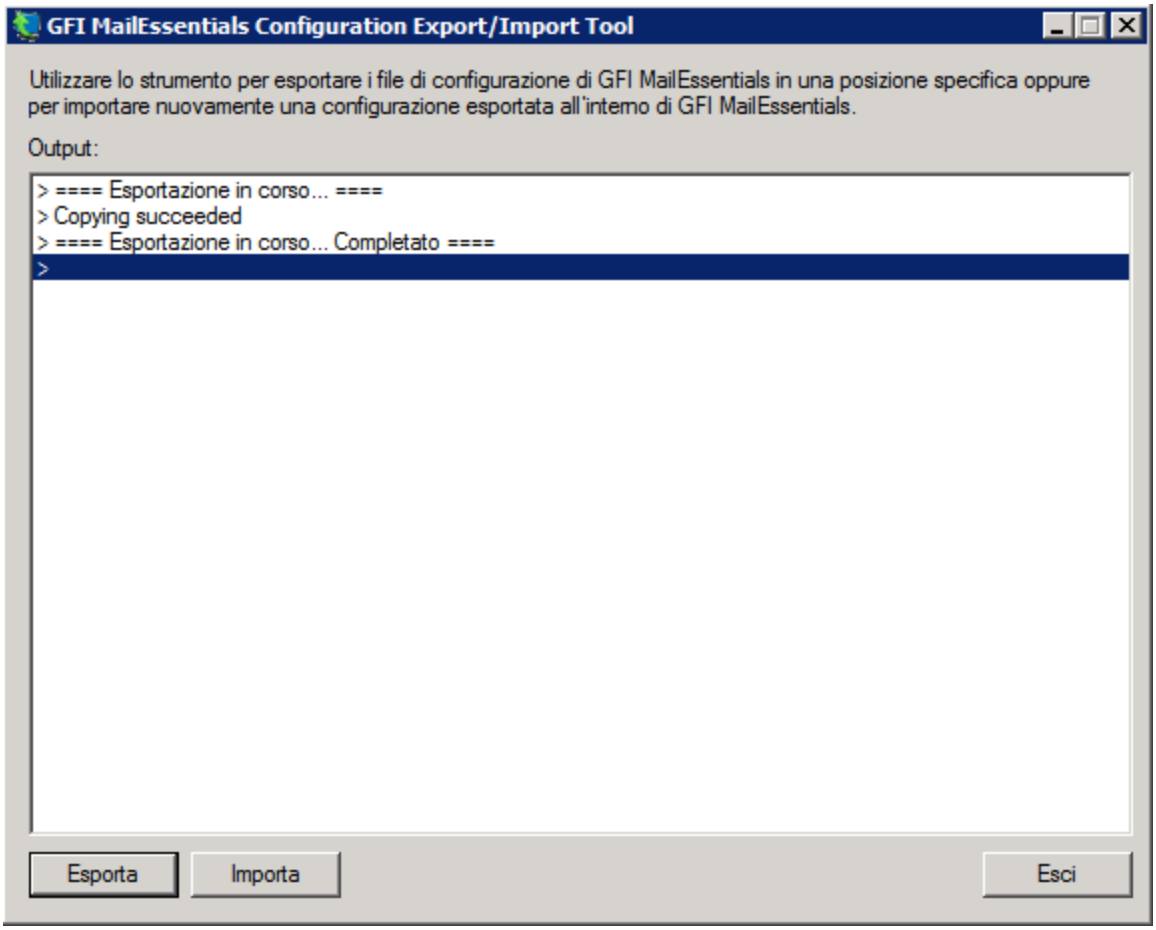
11.9.2 esportazione e importazione manuale delle impostazioni

GFI MailEssentials include un Strumento di esportazione/importazione di configurazione per l'esportazione delle impostazioni da un'installazione e l'importazione in un'altra.

> **NOTA**
> Le impostazioni possono anche essere importate e/o esportate dalla riga di comando. Per ulteriori informazioni, fare riferimento a Esportazione/importazione impostazioni dalla riga di comando (pagina 275).

Passaggio 1: Esportazione impostazioni esistenti

1. Andare a *<GFI MailEssentials percorso di installazione>*`\GFI\MailEssentials\` e avviare **meconfigmgr.exe**.


GFI MailEssentials Configuration Export/Import Tool
Utilizzare lo strumento per esportare i file di configurazione di GFI MailEssentials in una posizione specifica oppure per importare nuovamente una configurazione esportata all'interno di GFI MailEssentials.
Output:
> ==== Esportazione in corso... ====
> Copying succeeded
> ==== Esportazione in corso... Completato ====
>
Esporta
Importa
Esci

Schermata 144: strumento di esportazione/importazione di configurazione

> **NOTA**
> la durata del processo di esportazione dipende dalle dimensioni dei database.

4. Fare clic su **Esporta**.

5. Dalla finestra di dialogo **Sfoglia per cartelle**, selezionare la cartella dove esportare le impostazioni di configurazione, quindi fare clic su **OK**.

6. Al termine, fare clic su **Esci**.

Passaggio 2: copia delle impostazioni esportate

1. Copiare manualmente la cartella dove sono state esportate le impostazioni di configurazione.

2. Incollare la cartella nei computer dove è necessario importare le impostazioni.

Passaggio 3: importazione impostazioni in una nuova installazione

> **IMPORTANTE**
> Durante l'importazione delle impostazioni, i file importati sovrascriveranno le impostazioni esistenti (ad esempio, le impostazioni DNS di origine) e potrebbe essere necessario riconfigurare impostazioni di rete e azioni antispam specifiche.

NOTA
Durante l'esecuzione di questa operazione, alcuni servizi vengono arrestati temporaneamente. Questo potrebbe incidere sul flusso della posta e/o la scansione della posta.

1. Arrestare i servizi seguenti:

- GFI List Server
- GFI MailEssentials AS Scan Engine
- GFI MailEssentials Attendant
- GFI MailEssentials Autoupdater
- GFI MailEssentials AV Scan Engine
- GFI MailEssentials Backend
- Trasferimento Enterprise GFI MailEssentials
- GFI MailEssentials Legacy Attendant
- GFI MailEssentials Quarantine Action Services
- GFI POP2Exchange
- IIS Admin

2. Andare a *<GFI MailEssentials percorso di installazione>*\GFI\MailEssentials\ e avviare **meconfigmgr.exe**.

NOTA
La durata del processo di importazione dipende dalle dimensioni dei database da importare.

4. Fare clic su **Importa**, scegliere la cartella contenente i dati di importazione, quindi fare clic su **OK**.

AVVISO
Il processo di importazione sostituisce i file di configurazione con quelli presenti in questa cartella.

NOTA

Alcune delle impostazioni importate potrebbero non essere adatte all'installazione di GFI MailEssentials, pertanto può essere necessario riconfigurarle. Ciò è possibile, ad esempio, quando impostazioni DNS, elenco domini e server perimetrali sono diversi rispetto al server dal quale sono state esportate le impostazioni. Fare clic su **Sì** per avviare la procedura guidata di post-installazione di GFI MailEssentials e riconfigurare le impostazioni importanti.

Per ulteriori informazioni, fare riferimento a Procedura guidata di post-installazione (pagina 44).

È anche consigliato verificare le seguenti impostazioni che non sono state configurate nella procedura guidata di post-installazione.

» **Raccolta di directory**: deve essere verificato durante l'importazione in un server che si connette a un'Active Directory diversa o con un'Active Directory posizionata in un server diverso. Per ulteriori informazioni, fare riferimento a Raccolta di directory (pagina 115).

» **Operazioni spam**: alcune operazioni antispam sono disponibili solo per ambienti Microsoft® Exchange. Se si importano le impostazioni in un ambiente diverso (ad esempio, in un server IIS), le azioni non funzioneranno. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148).

NOTA

per ulteriori informazioni sulle impostazioni da verificare dopo l'importazione, fare riferimento a: http://go.gfi.com/?pageid=ME_CheckImportSettings

6. Al termine, fare clic su **Esci**.

7. GFI MailEssentials tenta il riavvio automatico dei servizi arrestati nel passaggio 1.

IMPORTANTE

Potrebbero esserci altri servizi arrestati al momento di interrompere il **Servizio Amministrazione di IIS**, come ad esempio il servizio **Simple Mail Transfer Protocol (SMTP)** . Riavviare manualmente questi servizi dall'applet Servizi.

11.9.3 Esportazione/importazione impostazioni dalla riga di comando

Esportazione impostazioni dalla riga di comando

1. Dal prompt dei comandi, cambiare directory selezionando la cartella principale di installazione di GFI MailEssentials.

2. Digitare:

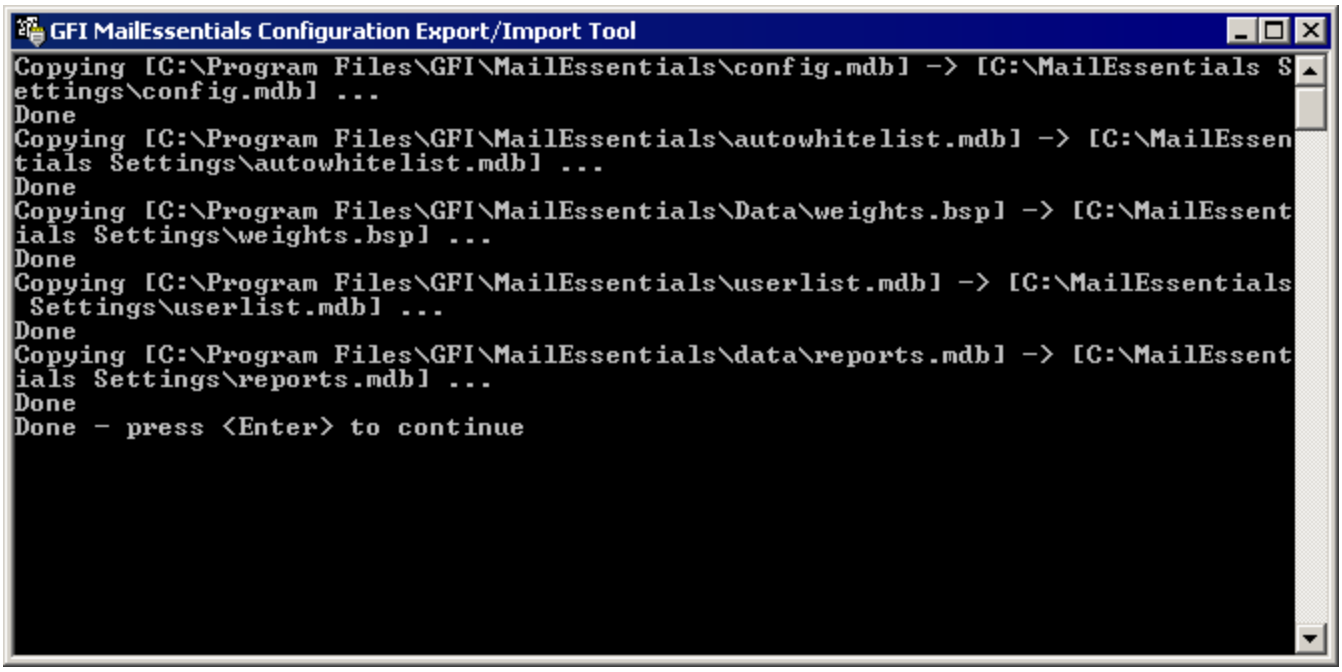
```
meconfigmgr /export:"c:\MailEssentials Settings" /verbose /replace
```

Dove:

» `"C:\MailEssentials Settings"`: percorso in cui esportare i file. Sostituire con il percorso di destinazione desiderato.

» `/verbose`: indica allo strumento di visualizzare l'avanzamento durante la copia dei file.

» `/replace`: indica allo strumento di sostituire i file esistenti nella cartella di destinazione.


GFI MailEssentials Configuration Export/Import Tool
Copying [C:\Program Files\GFI\MailEssentials\config.mdb] -> [C:\MailEssentials Settings\config.mdb] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\autowhitelist.mdb] -> [C:\MailEssentials Settings\autowhitelist.mdb] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\Data\weights.bsp] -> [C:\MailEssentials Settings\weights.bsp] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\userlist.mdb] -> [C:\MailEssentials Settings\userlist.mdb] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\data\reports.mdb] -> [C:\MailEssentials Settings\reports.mdb] ...
Done
Done - press <Enter> to continue

Schermata 145: esportazione impostazioni dalla riga di comando

3. Riavviare i servizi arrestati durante il passaggio 1.

Importazione impostazioni dalla riga di comando

1. Arrestare i servizi seguenti:

- GFI List Server
- GFI MailEssentials AS Scan Engine
- GFI MailEssentials Attendant
- GFI MailEssentials Autoupdater
- GFI MailEssentials AV Scan Engine
- GFI MailEssentials Backend
- Trasferimento Enterprise GFI MailEssentials
- GFI MailEssentials Legacy Attendant
- GFI MailEssentials Quarantine Action Services
- GFI POP2Exchange
- IIS Admin

2. Dal prompt dei comandi, cambiare directory selezionando la cartella principale di installazione di GFI MailEssentials.

3. Digitare:

```
meconfigmgr /import:"c:\MailEssentials Settings" /verbose /replace
```

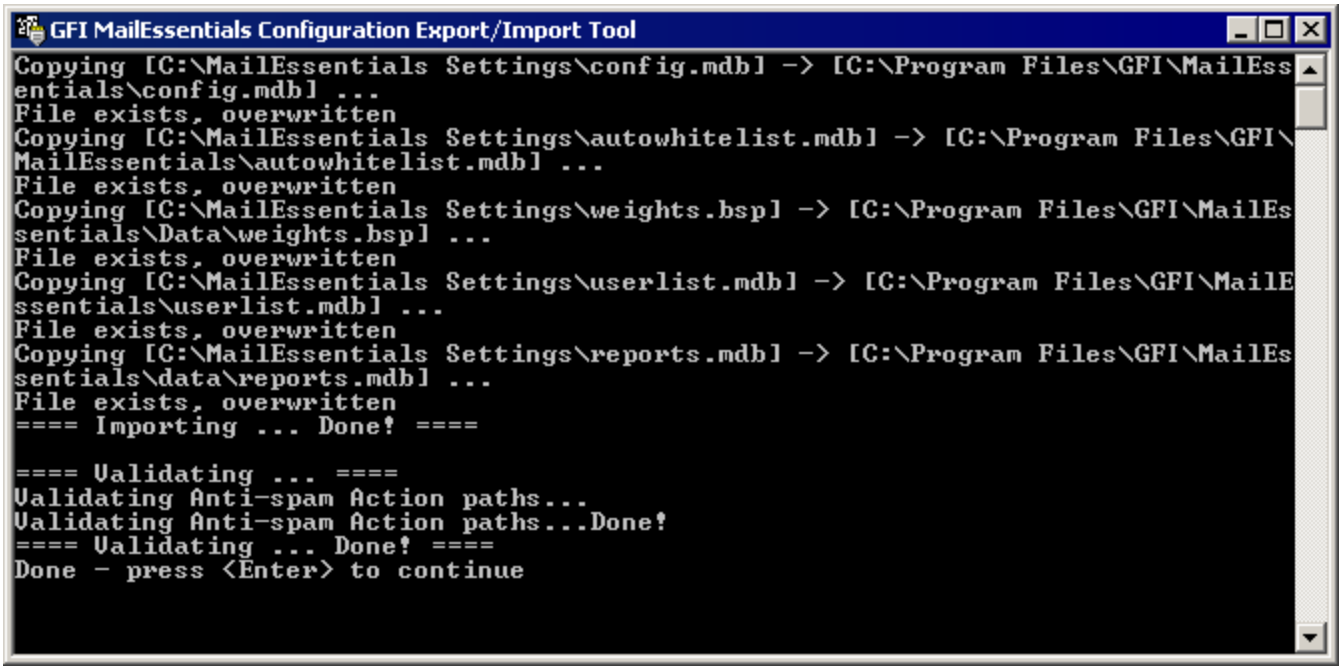
Dove:

- `"C:\MailEssentials Settings"`: percorso dei file da importare. Sostituire con il percorso in cui si trovano i file da importare.

» `/verbose`: indica allo strumento di visualizzare l'avanzamento durante la copia dei file.

» `/replace`: indica allo strumento di sostituire i file esistenti nella cartella di destinazione.

AVVISO
Il processo di importazione sostituisce i file di configurazione con quelli presenti in questa cartella.


GFI MailEssentials Configuration Export/Import Tool
Copying [C:\MailEssentials Settings\config.mdb] -> [C:\Program Files\GFI\MailEss
entials\config.mdb] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\autowhitelist.mdb] -> [C:\Program Files\GFI\
MailEssentials\autowhitelist.mdb] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\weights.bsp] -> [C:\Program Files\GFI\MailEs
sentials\Data\weights.bsp] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\userlist.mdb] -> [C:\Program Files\GFI\MailE
ssentials\userlist.mdb] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\reports.mdb] -> [C:\Program Files\GFI\MailEs
sentials\data\reports.mdb] ...
File exists, overwritten
==== Importing ... Done! ====
==== Validating ... ====
Validating Anti-spam Action paths...
Validating Anti-spam Action paths...Done!
==== Validating ... Done! ====
Done - press <Enter> to continue

Schermata 146: Importazione impostazioni dalla riga di comando

4. Riavviare i servizi arrestati durante il passaggio 1.

NOTA
Alcune delle impostazioni importate potrebbero non essere adatte all'installazione di GFI MailEssentials, pertanto può essere necessario riconfigurarle. Ciò è possibile, ad esempio, quando impostazioni DNS, elenco domini e server perimetrali sono diversi rispetto al server dal quale sono state esportate le impostazioni. Fare clic su **Sì** per avviare la procedura guidata di post-installazione di GFI MailEssentials e riconfigurare le impostazioni importanti.

Per ulteriori informazioni, fare riferimento a Procedura guidata di post-installazione (pagina 44).

È anche consigliato verificare le seguenti impostazioni che non sono state configurate nella procedura guidata di post-installazione.

» **Raccolta di directory**: deve essere verificato durante l'importazione in un server che si connette a un'Active Directory diversa o con un'Active Directory posizionata in un server diverso. Per ulteriori informazioni, fare riferimento a Raccolta di directory (pagina 115).

» **Operazioni spam**: alcune operazioni antispam sono disponibili solo per ambienti Microsoft® Exchange. Se si importano le impostazioni in un ambiente diverso (ad esempio, in un server IIS), le azioni non funzioneranno. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148).

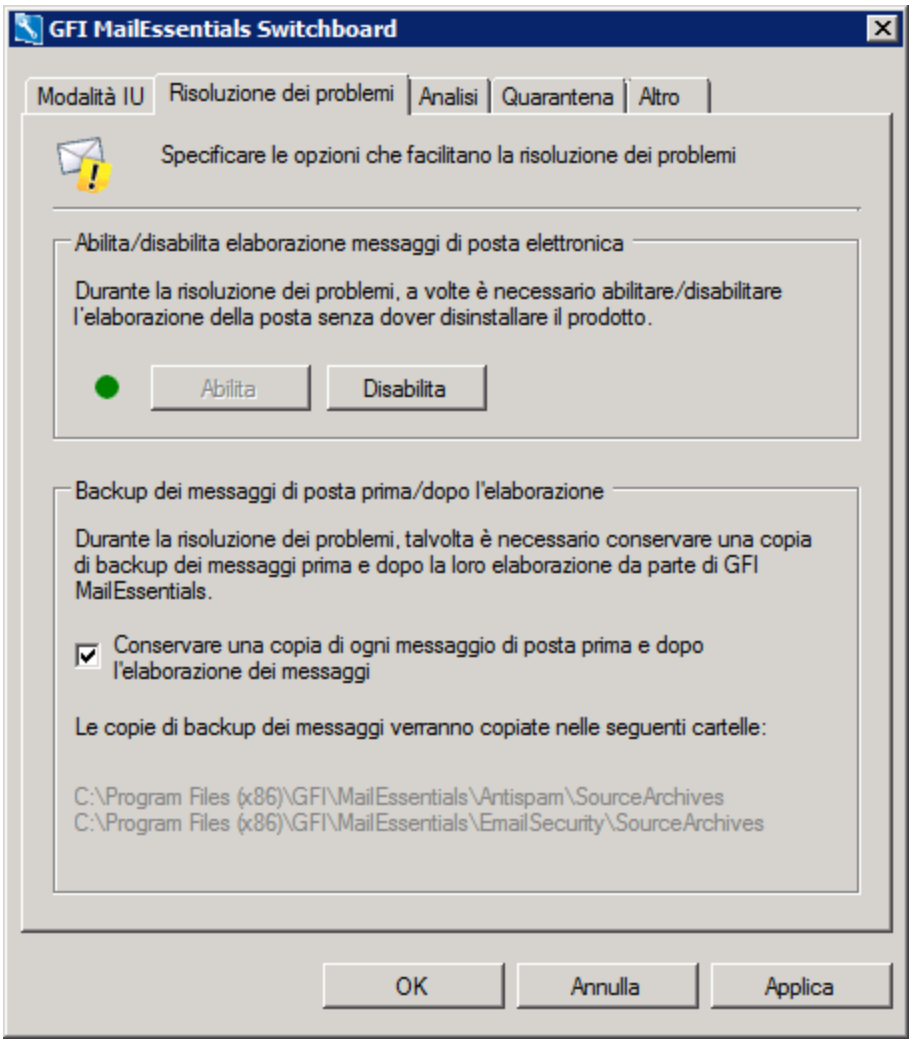
NOTA
Per ulteriori informazioni sulle impostazioni da verificare dopo l'importazione, fare riferimento a: http://go.gfi.com/?pageid=ME_CheckImportSettings

11.10 Disabilitazione elaborazione messaggi di posta elettronica

Disabilitando la protezione dell'elaborazione posta elettronica si disattiva l'intera protezione offerta da GFI MailEssentials e si permette il recapito dei messaggi nelle cassette postali degli utenti, compreso spam e messaggi dannosi. Normalmente l'elaborazione della posta viene disabilitata solo per la risoluzione dei problemi.

Per abilitare/disabilitare l'elaborazione dei messaggi in GFI MailEssentials:

1. Avviare GFI MailEssentials Switchboard da **Start > Tutti i programmi > GFI MailEssentials > Switchboard** e selezionare la scheda **Risoluzione dei problemi** .


GFI MailEssentials Switchboard
Modalità IU
Risoluzione dei problemi
Analisi
Quarantena
Altro
Specificare le opzioni che facilitano la risoluzione dei problemi
Abilita/disabilita elaborazione messaggi di posta elettronica
Durante la risoluzione dei problemi, a volte è necessario abilitare/disabilitare l'elaborazione della posta senza dover disinstallare il prodotto.
Abilita
Disabilita
Backup dei messaggi di posta prima/dopo l'elaborazione
Durante la risoluzione dei problemi, talvolta è necessario conservare una copia di backup dei messaggi prima e dopo la loro elaborazione da parte di GFI MailEssentials.
Conservare una copia di ogni messaggio di posta prima e dopo l'elaborazione dei messaggi
Le copie di backup dei messaggi verranno copiate nelle seguenti cartelle:
C:\Program Files (x86)\GFI\MailEssentials\Antispam\SourceArchives
C:\Program Files (x86)\GFI\MailEssentials\EmailSecurity\SourceArchives
OK
Annulla
Applica

Schermata 147: GFI MailEssentials Switchboard: Risoluzione dei problemi

2. Per abilitare o disabilitare l'elaborazione della posta, fare clic rispettivamente su **Abilita** o **Disabilita**.

NOTA
Durante l'esecuzione di questa operazione, alcuni servizi vengono arrestati temporaneamente. Questo potrebbe incidere sul flusso della posta e/o la scansione della posta.

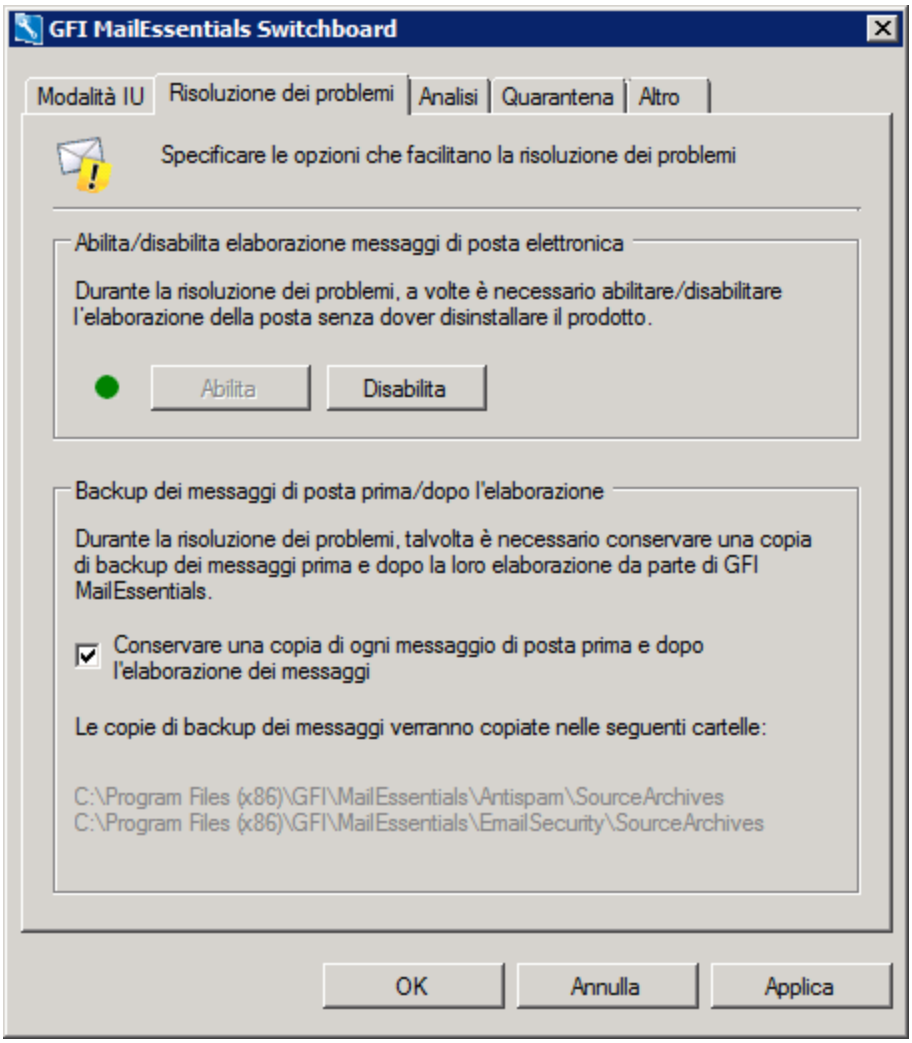
3. Nella finestra di dialogo **Necessario riavvio del servizio**, fare clic su **Sì** per riavviare i servizi.

4. Fare clic su **OK**.

11.11 Backup posta elettronica prima e dopo l'elaborazione

IMPORTANTE
Utilizzare questa opzione solo per la risoluzione dei problemi.

1. AvviareGFI MailEssentialsSwitchboard da **Start > Tutti i programmi > GFI MailEssentials > Switchboard** e selezionare la scheda **Risoluzione dei problemi** .


GFI MailEssentials Switchboard
Modalità IU
Risoluzione dei problemi
Analisi
Quarantena
Altro
Specificare le opzioni che facilitano la risoluzione dei problemi
Abilita/disabilita elaborazione messaggi di posta elettronica
Durante la risoluzione dei problemi, a volte è necessario abilitare/disabilitare l'elaborazione della posta senza dover disinstallare il prodotto.
Abilita
Disabilita
Backup dei messaggi di posta prima/dopo l'elaborazione
Durante la risoluzione dei problemi, talvolta è necessario conservare una copia di backup dei messaggi prima e dopo la loro elaborazione da parte di GFI MailEssentials.
Conservare una copia di ogni messaggio di posta prima e dopo l'elaborazione dei messaggi
Le copie di backup dei messaggi verranno copiate nelle seguenti cartelle:
C:\Program Files (x86)\GFI\MailEssentials\Antispam\SourceArchives
C:\Program Files (x86)\GFI\MailEssentials\EmailSecurity\SourceArchives
OK
Annulla
Applica

Schermata 148: GFI MailEssentials Switchboard: Risoluzione dei problemi

2. Selezionare la casella di controllo **Conservare una copia di ogni messaggio di posta prima e dopo l'elaborazione dei messaggi** per archiviare una copia di ciascun messaggio elaborato.

Tutti i messaggi sono archiviati nei percorsi seguenti:

» *<GFI MailEssentials percorso di installazione>*\GFI\MailEssentials\AntiSpam\SourceArchives\

» *<GFI MailEssentials percorso di installazione>*\GFI\MailEssentials\EmailSecurity\SourceArchives\

> **NOTA**
> Durante l'esecuzione di questa operazione, alcuni servizi vengono arrestati temporaneamente. Questo potrebbe incidere sul flusso della posta e/o la scansione della posta.

3. Fare clic su **OK**.

4. Nella finestra di dialogo **Necessario riavvio del servizio**, fare clic su **Sì** per riavviare i servizi.

5. Fare clic su **OK**.

11.12 Porte remote

Le porte remote permettono ai vari moduli di GFI MailEssentials di comunicare tra loro. Per impostazione predefinita, GFI MailEssentials utilizza le porte:

» **9090** - utilizzata dal servizio back-end diGFI MailEssentials

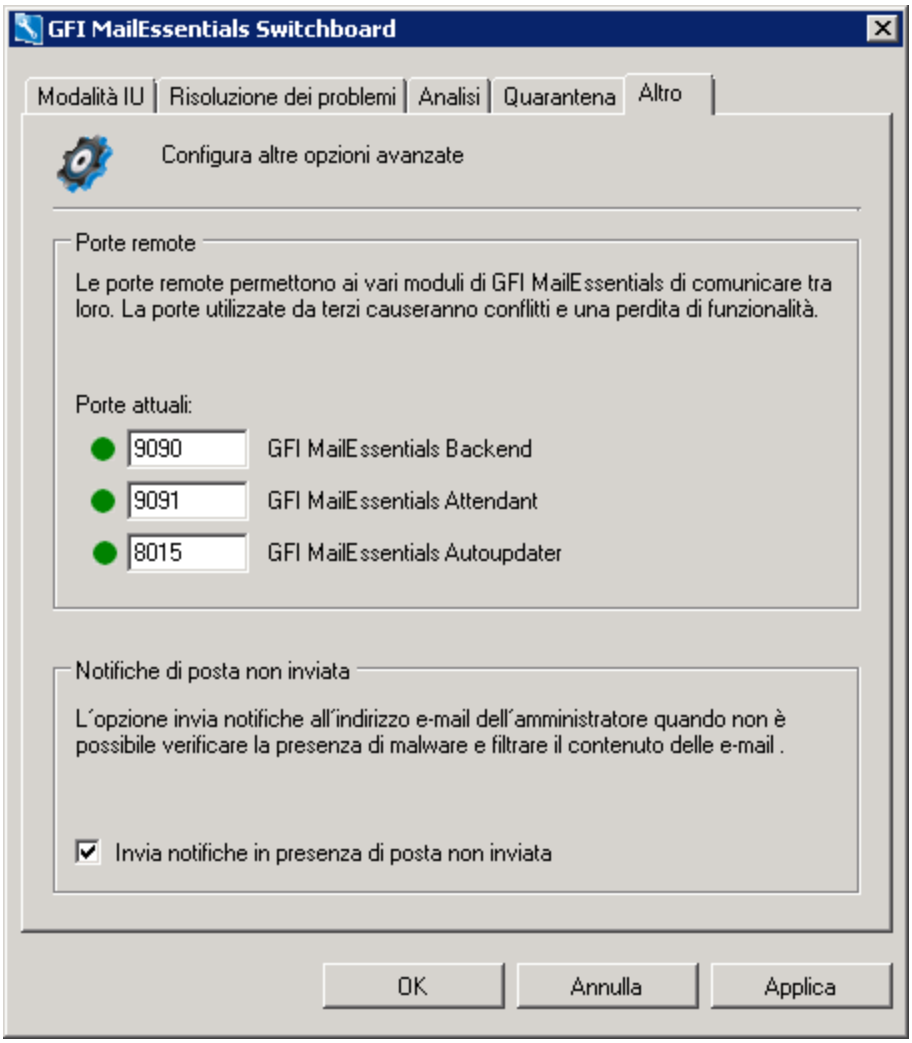
» **9091** - utilizzata da GFI MailEssentials Attendant service

» **8015** - utilizzata da GFI MailEssentials AutoUpdater service

Assicurarsi che non vi siano applicazioni in ascolto su queste porte, ad eccezione di GFI MailEssentials. Se queste porte vengono utilizzate da altre applicazioni, impostare numeri delle porte che non sono utilizzati dalle altre applicazioni.

Per modificare le porte remote:

1. Avviare GFI MailEssentials Switchboard da **Start > Tutti i programmi > GFI MailEssentials > Switchboard** e selezionare la scheda **Altro**.


GFI MailEssentials Switchboard
Modalità IU
Risoluzione dei problemi
Analisi
Quarantena
Altro
Configura altre opzioni avanzate
Porte remote
Le porte remote permettono ai vari moduli di GFI MailEssentials di comunicare tra loro. La porte utilizzate da terzi causeranno conflitti e una perdita di funzionalità.
Porte attuali:
9090
GFI MailEssentials Backend
9091
GFI MailEssentials Attendant
8015
GFI MailEssentials Autoupdater
Notifiche di posta non inviata
L´opzione invia notifiche all´indirizzo e-mail dell´amministratore quando non è possibile verificare la presenza di malware e filtrare il contenuto delle e-mail .
Invia notifiche in presenza di posta non inviata
OK
Annulla
Applica

Schermata 149: modifica delle porte remote

2. Nell'area **Porte remote**, modificare il numero della porta remota con un altro che non viene utilizzato dalle altre applicazioni.

3. Fare clic su **Applica**.

> **NOTA**
> Durante l'esecuzione di questa operazione, alcuni servizi vengono arrestati temporaneamente. Questo potrebbe incidere sul flusso della posta e/o la scansione della posta.

4. Per eseguire il riavvio dei servizi visualizzati, fare clic su **Sì**.

5. Fare clic su **OK**.

11.13 Monitoraggio API di scansione antivirus

Quando GFI MailEssentials viene installato su un computer Microsoft® Exchange, è possibile monitorare le prestazioni dell'API di scansione antivirus utilizzando Performance Monitor MCC.

NOTA
Information Store Protection (VSAPI) non è supportato su Microsoft® Exchange Server 2013, in quanto VSAPI è stato rimosso da Microsoft® Exchange Server 2013.

11.13.1 Contatore di prestazioni in Windows 2003 Server

Per aggiungere e visualizzare il contatore di performance monitor in Windows 2003 Server, attenersi alla seguente procedura:

1. Fare clic su **Start > Pannello di controllo**.

2. Nella finestra del Pannello di controllo, fare doppio clic su **Strumenti di amministrazione**.

3. Fare doppio clic su **Performance** per avviare la MMC di **Performance monitor**.

4. Dal riquadro di visualizzazione **Monitor di sistema**, fare clic su **Aggiungi** per caricare la finestra di dialogo **Aggiungi contatori**.

5. Dall'elenco a discesa **Oggetto prestazione**, selezionare **MSExchangeIS**.

6. Fare clic su **Seleziona i contatori dall'elenco**.

7. Selezionare uno dei contatori di **scansione virus** da aggiungere. Per ulteriori informazioni, fare riferimento a Contatori di performance monitor (pagina 284).

8. Fare clic su **Aggiungi**.

9. Per aggiungere tutti i contatori di prestazioni necessari, ripetere i passaggi 7 e 8.

10. Fare clic su **Chiudi**.

Adesso i contatori dei processi aggiunti vengono visualizzati in Performance Monitor.

11.13.2 Contatore di prestazioni in Windows 2008 Server

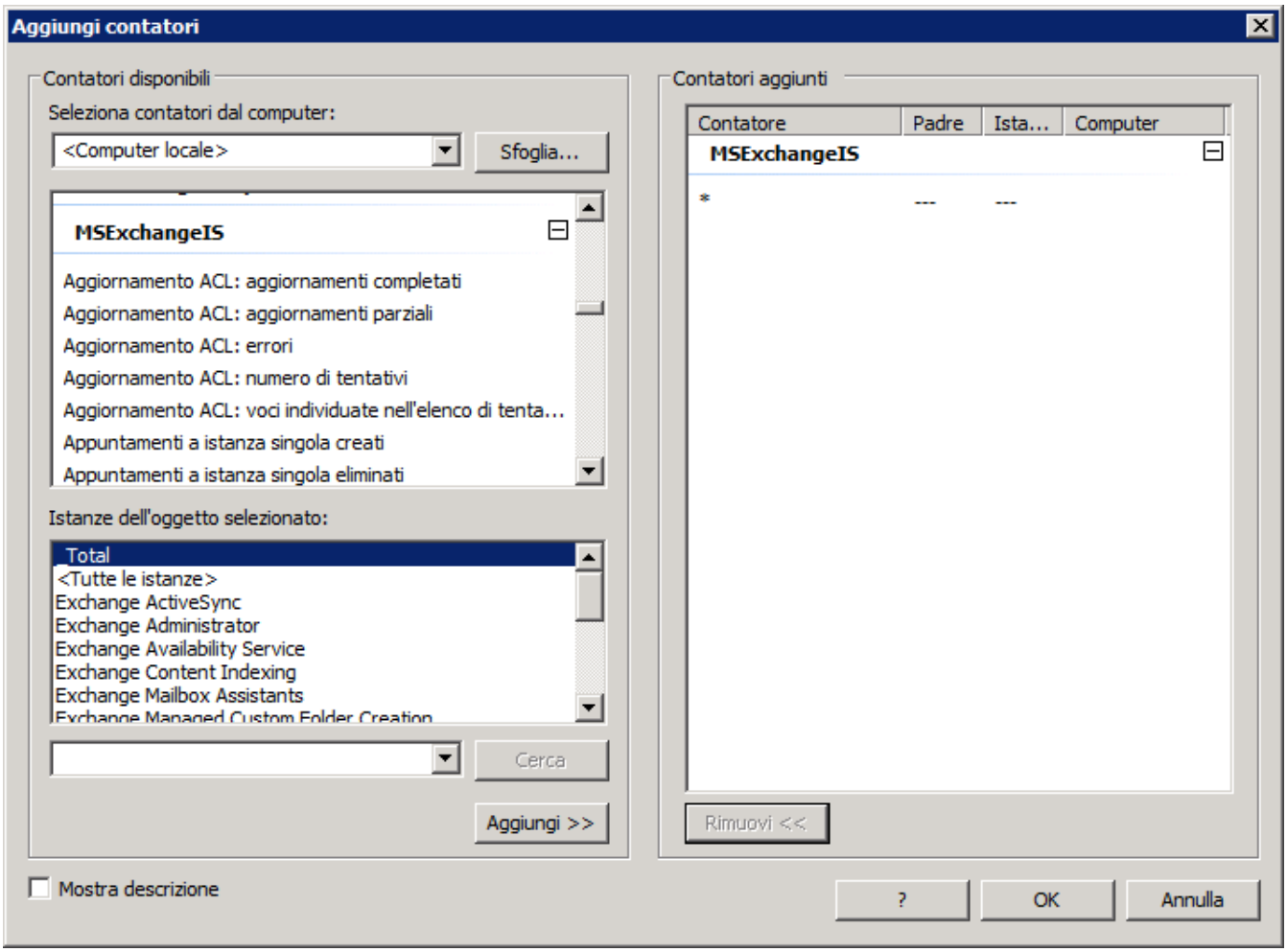
NOTA
In un ambiente Microsoft® Exchange Server 2007/2010, i contatori di monitor delle prestazioni VSAPI sono disponibili solo sui computer dove è installato il ruolo server cassetta postale.

Per aggiungere e visualizzare il contatore di performance monitor in Windows 2008 Server, attenersi alla seguente procedura:

1. Accedere a **Pannello di controllo > Strumenti di amministrazione > Monitoraggio affidabilità e Performance Monitor.**

2. Nella finestra di dialogo del monitor, espandere **Strumenti di monitoraggio** e selezionare **Performance Monitor**.

3. Dal riquadro di visualizzazione, fare clic su **Aggiungi** per caricare la finestra di dialogo **Aggiungi contatori**.



Schermata 150: aggiunta di contatori di performance monitor VSAPI a Windows 2008 Server

4. Dall'elenco a discesa **Seleziona contatori dal computer**, scegliere il computer da monitorare.

5. Dall'elenco di contatori disponibili, espandere **MSExchangeIS**.

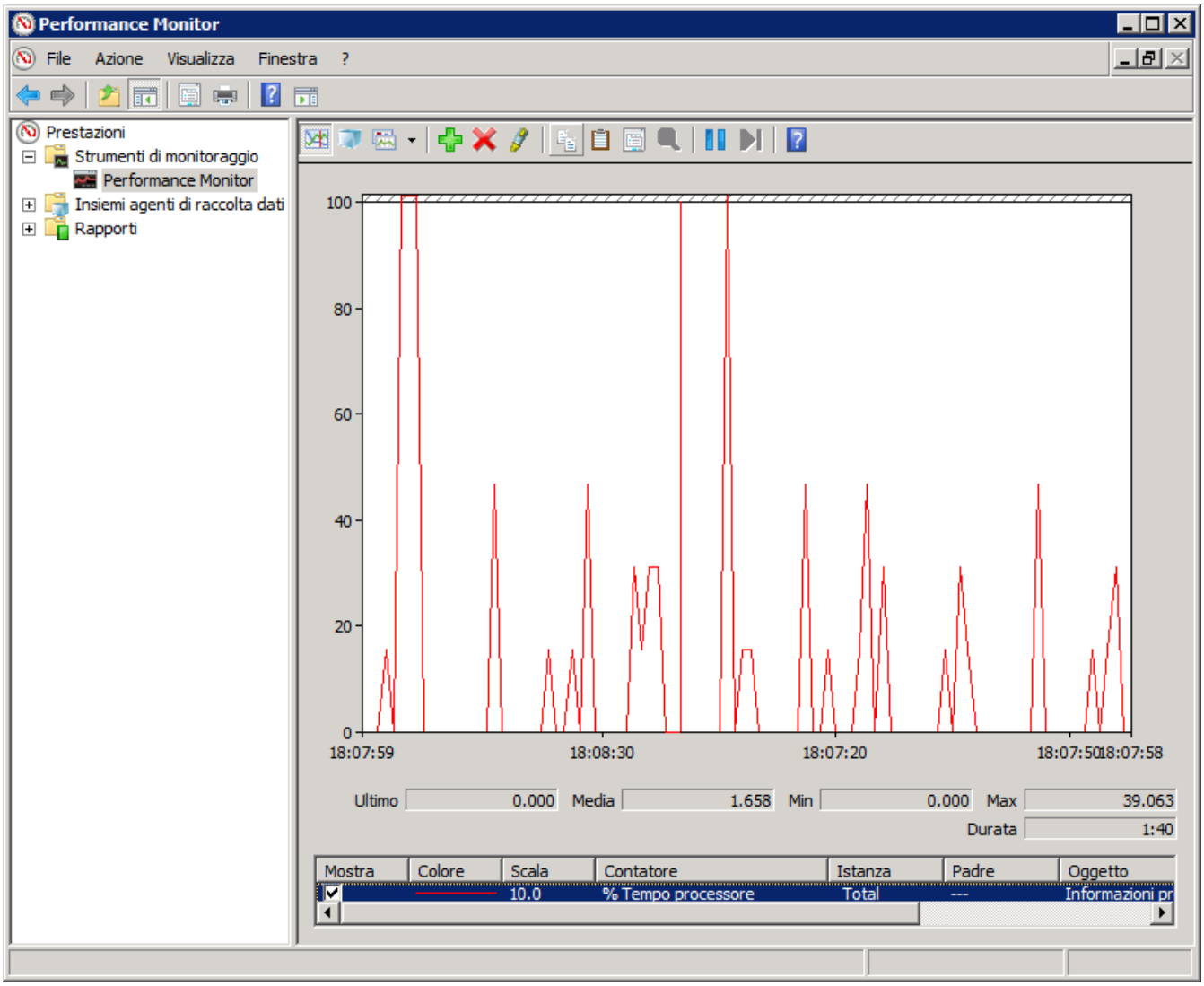
6. Selezionare uno dei contatori di **scansione virus** da aggiungere. Per ulteriori informazioni, fare riferimento a Contatori di performance monitor (pagina 284).

7. Fare clic su **Aggiungi**.

8. Ripetere i passaggi 6 e 7 per ciascun processo da monitorare.

9. Per applicare le modifiche fare clic su **Ok**.

Adesso i contatori dei processi aggiunti vengono visualizzati in Performance Monitor.



Schermata 151: monitoraggio file di scansione antivirus scansionati nel performance monitor di Windows Server 2008

11.13.3 Contatori di performance monitor

Sono disponibili i seguenti contatori di Performance Monitor VSAPI:

Contatore di prestazioni	Descrizione
Messaggi elaborati da ricerca virus	Un valore cumulativo del numero totale di messaggi di livello superiore elaborati dal programma di scansione antivirus.
Numero messaggi elaborati/sec	Rappresenta la frequenza con cui i messaggi di livello superiore vengono elaborati dal programma antivirus.
Messaggi puliti da ricerca virus	Numero totale dei messaggi di livello superiore puliti dal programma antivirus.
Messaggi puliti/sec	La frequenza con cui i messaggi di livello superiore vengono puliti dal programma antivirus.
Messaggi messi in quarantena da ricerca virus	Numero totale dei messaggi di livello superiore messi in quarantena dal programma antivirus.
Messaggi messi in quarantena/sec	La frequenza con cui i messaggi di livello superiore vengono messi in quarantena dal programma antivirus.
File analizzati da ricerca virus	Numero totale di messaggi di livello superiore elaborati dal programma di scansione antivirus.

Contatore di prestazioni	Descrizione
File analizzati/sec	Frequenza con cui i singoli file vengono elaborati dal programma antivirus.
File puliti da ricerca virus	Numero totale dei singoli file puliti dal programma antivirus.
File puliti/sec	La frequenza con cui i singoli file vengono puliti dal programma antivirus.
File messi in quarantena da ricerca virus	Numero totale dei singoli file messi in quarantena dal programma antivirus.
File messi in quarantena/sec	Frequenza con cui i singoli file vengono messi in quarantena dal programma antivirus.
Byte analizzati da ricerca virus	Numero totale di byte in tutti i file elaborati dal programma di scansione antivirus.
Lunghezza coda ricerca virus	Numero corrente di richieste in sospeso accodate per la ricerca virus.
Cartelle analizzate da ricerca virus in background	Numero totale di cartelle elaborate dal programma antivirus in background.
Messaggi analizzati da ricerca virus in background	Numero totale di messaggi elaborati dal programma antivirus in background.

12 Risoluzione dei problemi e supporto

12.1 Introduzione

In questo capitolo viene spiegato come risolvere i problemi che si possono verificare durante l'installazione di GFI MailEssentials. Le principali fonti di informazioni disponibili per la risoluzione dei problemi sono:

» Il presente manuale. La maggior parte dei problemi può essere risolta leggendo le informazioni contenute nella sezione di questo manuale.

» Gli articoli di GFI Knowledge Base

» Forum Web

» Il reparto di assistenza tecnica di GFI

12.2 Problemi comuni

Problema rilevato	Soluzione
Il Dashboard mostra che non vi è alcun messaggio in elaborazione; oppure, Vengono elaborati solo i messaggi in entrata o in uscita	1. Assicurarsi che in GFI MailEssentials non sia disabilitata la scansione dei messaggi. Per ulteriori informazioni, fare riferimento a Disabilitazione elaborazione messaggi di posta elettronica (pagina 278). 2. Controllare la presenza di server virtuali SMTP IIS Microsoft® e assicurarsi che GFI MailEssentials sia associato al server virtuale corretto. Per ulteriori informazioni, fare riferimento a Binding server virtuale SMTP (pagina 246). 3. Il record MX del dominio non è configurato correttamente. Accertarsi che il record MX indichi l'indirizzo IP del server che esegue GFI MailEssentials. 4. Se i messaggi in entrata passano attraverso un altro gateway, accertarsi che il server di posta in esecuzione su di esso esegua l'inoltro dei messaggi in entrata attraverso GFI MailEssentials. 5. Accertarsi che i messaggi in uscita siano configurati per l'inoltro tramite GFI MailEssentials. Per ulteriori informazioni, fare riferimento a Installazione in un gateway di posta o su un relay server/server perimetrale (pagina 26). 6. Verificare che il server virtuale SMTP utilizzato da Microsoft® Exchange Server per i messaggi in uscita sia il medesimo server SMTP a cui è associato GFI MailEssentials. Per ulteriori informazioni su come risolvere questo problema, fare riferimento a: http://go.gfi.com/?pageid=ME_MonitorProcessing
Dopo l'installazione di GFI MailEssentials, alcuni messaggi mostrano un corpo dell'oggetto distorto durante la visualizzazione in Microsoft® Outlook	Questo problema si verifica nei messaggi che utilizzano più di un set di caratteri per l'intestazione del messaggio e un set di caratteri diverso per il corpo. Quando questi messaggi vengono elaborati da Microsoft® Exchange 2003, verranno visualizzati distorti in Microsoft® Outlook. Per risolvere questo problema, Microsoft® ha rilasciato un hotfix. Per ulteriori informazioni, fare riferimento a: http://go.gfi.com/?pageid=ME_OutlookCharacters and http://go.gfi.com/?pageid=ME_MessageGarbled

Problema rilevato	Soluzione
GFI MailEssentials è configurato per spostare in una cartella secondaria della cassetta postale degli utenti i messaggi bloccati come SPAM. I client connessi a Microsoft® Exchange tramite POP3 non sono in grado di visualizzare i messaggi bloccati come SPAM.	Connettersi a Microsoft® Exchange tramite IMAP. per ulteriori informazioni, fare riferimento a: http://go.gfi.com/?pageid=ME_POP3ViewSpam
Gli aggiornamenti automatici non vengono eseguiti, anche se funziona correttamente il download manuale effettuato dalla configurazione di GFI MailEssentials	Assicurarsi che siano consentite le connessioni non autenticate dal computer di GFI MailEssentials a http://update.gfi.com sulla porta 80. per ulteriori informazioni, fare riferimento a: http://go.gfi.com/?pageid=ME_AutoUpdatesFail Se applicabile, controllare anche il server proxy.
Impossibile importare i dati di configurazione.	Assicurarsi che la versione e build di GFI MailEssentials sia identica tra le installazioni di origine e di destinazione. Per ulteriori informazioni su come risolvere questo problema, fare riferimento a: http://go.gfi.com/?pageid=ME_ExpImpBuild
I comandi remoti non funzionano	Fare riferimento all'articolo: http://go.gfi.com/?pageid=ME_RemoteCommands
L'elaborazione dei messaggi di posta è molto lenta.	Questo può verificarsi quando vi sono problemi DNS nella rete. Se il DNS non funziona correttamente, si verificherà il timeout delle ricerche DNS eseguite da alcuni filtri antispam di GFI MailEssentials. Per ulteriori informazioni, fare riferimento a: http://go.gfi.com/?pageid=ME_ProcessingSlow
I dati precedenti non sono disponibili nel database quando si utilizza Microsoft® Access.	Quando il database **reports.mdb** supera 1,7 GB, si rinomina automaticamente in **reports_<date>.mdb** e viene creato un nuovo database **reports.mdb**. Per ulteriori informazioni su come risolvere questo problema, fare riferimento a: http://go.gfi.com/?pageid=ME_ReportDB
L'interfaccia della quarantena visualizza l'errore D10 - **Impossibile accedere al database Quarantine Store. Utilizzare uno strumento di riparazione del database come esentutl.exe.**	Per ulteriori informazioni sull'utilizzo di esentutl.exe per la riparazione del database Quarantine Store, fare riferimento a http://go.gfi.com/?pageid=ME_esentutl.
Errore durante la ricezione di messaggi di posta: **Tipo corpo non supportato dall'host remoto**	Questo errore si verifica quando i messaggi di posta vengono inoltrati dal server SMTP di IIS al server Microsoft® Exchange. Ciò si verifica perché le versioni 4.0, 5.0 e 5.5 di Microsoft® Exchange Server non sono in grado di gestire i messaggi MIME a 8 bit. Per istruzioni sulla disattivazione di 8BITMIME in Windows Server 2003, fare riferimento a: http://go.gfi.com/?pageid=ME_TurnOff8bitMIME.
I messaggi attendibili vengono spostati nella cartella **failedmails**	**Causa** Quando GFI MailEssentials non è in grado di scansionare i messaggi in entrata, questi non sono recapitati ai destinatari dato che contengono contenuto dannoso. GFI MailEssentials sposta i messaggi nella seguente cartella: <*GFI MailEssentials percorso di installazione*>\GFI\MailEssentials\EmailSecurity\failedmails\ **Soluzione** Se i messaggi attendibili vengono spostati nella cartella failedmails, questi possono essere rielaborati manualmente per la consegna. Per ulteriori informazioni, fare riferimento a Messaggi di posta elettronica non riusciti (pagina 256). Per ulteriori informazioni sui messaggi non riusciti, fare riferimento a: http://go.gfi.com/?pageid=ME_FailedMails

Problema rilevato	Soluzione
Devo aggiornare il codice di licenza quando passo alla nuova versione?	Le informazioni sulla gestione licenze sono disponibili all'indirizzo: http://go.gfi.com/?pageid=ME_adminManualEN
Dove si trova la versione online di questo manuale?	La versione online di questo manuale è disponibile all'indirizzo: http://go.gfi.com/?pageid=GFI_Manuals

12.3 Motori e filtri di scansione

Problema rilevato	Soluzione
Lo spam viene recapitato nella cassetta postale degli utenti	Per risolvere questo problema, attenersi all'elenco di controllo sottostante: 1. Verificare che in GFI MailEssentials non sia disabilitata la scansione dei messaggi. Per ulteriori informazioni, fare riferimento a Disabilitazione elaborazione messaggi di posta elettronica (pagina 278). 2. Controllare che siano abilitati tutti i filtri necessari. Per ulteriori informazioni, fare riferimento a Filtri antispam (pagina 109). 3. Controllare che i domini locali siano configurati correttamente. Per ulteriori informazioni, fare riferimento a Domini locali (pagina 244). 4. Controllare che i messaggi passino attraverso GFI MailEssentials oppure che GFI MailEssentials sia associato al server SMTP virtuale di IIS corretto. 5. Controllare che il percorso '%TEMP%' (per impostazione predefinita è la cartella 'C:\Windows\Temp') non contenga molti file. 6. Controllare se il numero degli utenti che utilizza GFI MailEssentials supera il numero delle licenze acquistate. 7. Controllare se la whitelist è configurata correttamente. Per ulteriori informazioni, fare riferimento a Whitelist (pagina 141). 8. Controllare che le azioni siano configurate correttamente. Per ulteriori informazioni, fare riferimento a Operazioni antispam - cosa fare con lo spam. (pagina 148). 9. Controllare se il filtro di analisi bayesiana è configurato correttamente. Per ulteriori informazioni, fare riferimento a Analisi bayesiana (pagina 138). Per ulteriori informazioni su come risolvere questo problema, fare riferimento a: http://go.gfi.com/?pageid=ME_SpamChecklist
Le pagine Block list e-mail, Whitelist e/o Filtro contenuti richiedono troppo tempo a caricare o si bloccano	Limitare il numero di voci negli elenchi a 10.000.
Gli aggiornamenti di SpamRazer non vengono scaricati	1. Accertarsi che il codice di licenza sia valido. 2. Assicurarsi che siano aperte le porte necessarie e che il firewall sia configurato per consentire le connessioni dal server GFI MailEssentials. Per ulteriori informazioni, fare riferimento a Impostazioni delle porte del firewall (pagina 25). 3. Assicurarsi che, ove applicabili, le impostazioni del server proxy per la connessione a Internet siano corrette.

Problema rilevato	Soluzione
I messaggi di posta non vengono inseriti nella greylist.	Per verificare il funzionamento della greylist: **Passaggio 1: conferma abilitazione greylist** Dalle proprietà della greylist, assicurarsi di avere selezionato Abilita greylist. **Passaggio 2: verifica indirizzi esclusi** Nelle esclusioni IP ed e-mail delle proprietà greylist, assicurarsi che non vi siano esclusioni errate (come *@*.com). **Passaggio 3: utilizzare esentutl.exe per verificare che il database della greylist non sia danneggiato** Per maggiori informazioni, fare riferimento a: http://go.gfi.com/?pageid=ME_esentutl
Ricezione di messaggi spam dal proprio dominio.	Alcuni messaggi spam contengono un indirizzo e-mail falso "SMTP FROM", costituito dallo stesso dominio del destinatario. In tal modo, potrebbe sembrare che il messaggio provenga da un utente locale. 1. Abilitare il filtro Sender Policy Framework dal filtro antispam di SpamRazer per il blocco dei messaggi di posta provenienti da indirizzi contraffatti. Per ulteriori informazioni, fare riferimento a SpamRazer (pagina 110). 2. Creare un record SPF per il proprio dominio. Per ulteriori informazioni, fare riferimento a http://go.gfi.com/?pageid=ME_CreateSPFRecord. 3. Assicurarsi SpamRazer sia configurato per l'esecuzione a una priorità superiore rispetto al modulo Whitelist. Per ulteriori informazioni, fare riferimento a Ordinamento filtri antispam in base alla priorità. (pagina 151).
I messaggi inviati dai mittenti inseriti nella whitelist sono bloccati.	1. I messaggi inseriti nella whitelist possono essere bloccati se presentano contenuto o allegati che violano le regole antimalware, poiché queste hanno una priorità superiore rispetto alla whitelist. Accertarsi che i messaggi bloccati non violino le regole antimalware. 2. Assicurarsi che le priorità del filtro siano impostate in modo che la whitelist sia più importante di qualsiasi altro filtro applicato alla posta desiderata. Per ulteriori informazioni, fare riferimento a: http://go.gfi.com/?pageid=ME_BlockedWhitelistedSenders
Spam non recapitato nella cartella secondaria di Microsoft® Exchange o spam non recapitato nella cartella secondaria prevista di Outlook in un ambiente Microsoft® Exchange Server 2010	1. Confermare che questa funzione sia configurata correttamente. Per ulteriori informazioni, fare riferimento a Spostamento spam nella cartella di Exchange 2010 (pagina 266). 2. Per informazioni dettagliate sulla risoluzione di questo problema, fare riferimento a http://go.gfi.com/?pageid=ME_AutodiscoverIssues.

12.4 Gestione posta elettronica

Problema rilevato	Soluzione
Non viene aggiunta nessuna liberatoria ai messaggi in uscita.	Le liberatorie vengono aggiunte solo ai messaggi in uscita provenienti da domini protetti da GFI MailEssentials. Le liberatorie non vengono aggiunte quando: » I messaggi vengono inviati da domini che non sono specificati nell'elenco domini locali. » I messaggi vengono inviati a domini che si trovano nell'elenco domini locali, poiché questi verranno considerati come messaggi di posta interni. Assicurarsi che tutti i domini locali siano specificati nella finestra di dialogo Domini di posta elettronica in arrivo. Per ulteriori informazioni, fare riferimento a Domini locali (pagina 244).

Problema rilevato	Soluzione
Alcuni caratteri nella dichiarazione di non responsabilità non sono visualizzati correttamente.	Configurare Microsoft® Outlook per non utilizzare la codifica automatica e forzare GPO a utilizzare la codifica corretta. Per ulteriori informazioni su come risolvere questo problema, fare riferimento a: http://go.gfi.com/?pageid=ME_Outlook2003Encoding
I messaggi inviati al server di elenco vengono convertiti in testo normale	I messaggi inviati al server di elenco vengono convertiti in testo normale solo quando il formato originale del messaggio è RTF. Inviare il messaggio in formato HTML per mantenere il formato originale.
Gli utenti interni ricevono un rapporto di mancato recapito quando inviano la posta al server di elenco e GFI MailEssentials è installato in un computer gateway	Per ulteriori informazioni su come utilizzare la funzione server di elenco quando GFI MailEssentials è installato in un gateway, fare riferimento a: http://go.gfi.com/?pageid=ME_ListServerGateway
I messaggi inviati o destinati a determinati utenti non vengono monitorati.	Le regole di monitoraggio della posta non monitorano i messaggi provenienti o destinati all'amministratore di GFI MailEssentials e l'indirizzo di posta elettronica a cui vengono inviati i messaggi monitorati. Le regole di monitoraggio della posta non sono inoltre applicabili ai messaggi inviati tra gli utenti interni del medesimo archivio informazioni.

12.5 GFI SkyNet

GFI cura la gestione di una Knowledge Base completa contenente le risposte ai problemi più comuni. GFI SkyNet contiene sempre l'elenco più aggiornato delle domande e delle patch fornite dal supporto tecnico. Se le informazioni contenute nella presente guida non risolvono i problemi, fare riferimento a GFI SkyNet all'indirizzo: http://kb.gfi.com/.

12.6 Forum Web

L'assistenza tecnica tra utenti è disponibile sul forum Web di GFI. Il forum Web è disponibile all'indirizzo: http://forums.gfi.com/.

12.7 Richiesta di supporto tecnico

Se nessuna delle risorse precedenti ha permesso di risolvere i problemi, contattare il personale di assistenza tecnica di GFI compilando il modulo di richiesta online o telefonando.

» **Online**: Compilare il modulo di richiesta di supporto e seguire rigorosamente le istruzioni indicate nella pagina per inviare la richiesta: http://support.gfi.com/supportrequestform.asp

» **Telefono**: Per ottenere il numero telefonico corretto dell'assistenza tecnica della regione competente, visitare il sito: http://www.gfi.com/company/contact.htm

> **NOTA**
> Prima di contattare l'assistenza tecnica, accertarsi di avere a disposizione l'ID cliente. L'ID cliente è il numero dell'account cliente online assegnato alla prima registrazione delle chiavi di licenza nell'Area clienti GFI alla pagina http://customers.gfi.com.

Il team risponderà alla richiesta entro 24 ore al massimo, a seconda del fuso orario.

12.8 Documentazione

Se questo manuale non soddisfa le attese o si ritiene che possa in qualche modo essere migliorato, inviare un messaggio di posta elettronica a: documentation@gfi.com.

13 Appendice - Filtro bayesiano

Il filtro bayesiano è una tecnologia antispam utilizzata all'interno di GFI MailEssentials. È una tecnologia adattiva basata su algoritmi di intelligenza artificiale, rafforzata per contrastare la più ampia gamma di tecniche di spamming attualmente disponibili.

Il presente manuale illustra il funzionamento del filtro bayesiano, oltre alla modalità di configurazione e di addestramento dello stesso.

> **NOTA**
> 1. Il filtro antispam bayesiano è disabilitato per impostazione predefinita. Prima di abilitare il filtro bayesiano, si consiglia di addestrarlo.
> 2. GFI MailEssentials deve essere attivo per almeno una settimana affinché il filtro bayesiano raggiunga la piena operatività. È necessario eseguire tale operazione preliminare, dato che il filtro bayesiano raggiunge il tasso massimo di rilevazione quando si adatta alla struttura della posta dell'utente.

Funzionamento del filtro antispam bayesiano

Il filtro bayesiano è basato sul principio che la maggioranza degli eventi siano dipendenti tra loro e che la probabilità del verificarsi di un evento futuro può essere dedotta dalle occorrenze precedenti di quell'evento.

> **NOTA**
> Consultare i collegamenti sottostanti per ulteriori informazioni sulla base matematica del filtro bayesiano:
> http://go.gfi.com/?pageid=ME_BayesianParameterEstimation

La medesima tecnologia è stata adattata da GFI MailEssentials per l'identificazione e classificazione dello spam. Se un frammento di testo viene spesso visualizzato nei messaggi spam ma non in quelli attendibili, è ragionevole desumere che il messaggio in questione sia probabilmente spam.

Creazione di un database personalizzato di parole bayesiane

Prima di utilizzare il filtro bayesiano, è necessario creare un database con parole e token (ad esempio il segno $, gli indirizzi IP e i domini ecc.). Può essere raccolto da un campione di messaggi spam e posta attendibile, detta 'ham'.

Viene quindi assegnato un valore di probabilità a ciascuna parola o token, sulla base di calcoli che tengono presente la frequenza delle parole nello spam rispetto allo ham. Ciò è il risultato dell'analisi della posta in uscita e dello spam noto degli utenti: tutte le parole e i token dei due pool di messaggi vengono analizzati per generare la probabilità che una particolare parola indichi che il messaggio è spam.

Tale probabilità è calcolata in base al seguente esempio:

Se la parola 'mutuo' è presente in 400 messaggi spam su 3.000 e su 5 messaggi di posta attendibile su 300, allora la probabilità che sia spam è dello 0,8889 (ad es. [400/3000] / [5/300 + 400/3000]).

Creazione di un database personalizzato della posta ham

L'analisi dei messaggi spam viene effettuata sulla posta dell'azienda, pertanto è realizzata su misura.

» **Esempio:** Un istituto finanziario potrebbe usare spesso la parola ‘mutuo’ e otterrebbe molti falsi positivi se utilizzasse una serie di regole antispam generiche. D’altra parte, il filtro bayesiano, se personalizzato per la propria azienda dopo un periodo di addestramento iniziale, prende nota della posta in uscita valida dell’azienda (riconoscendo ‘mutuo’ come spesso presente nei messaggi attendibili), dunque avrà una percentuale di rilevazione spam molto migliore e una percentuale assai inferiore di falsi positivi.

Creazione del database spam bayesiano

A parte la posta ham, il filtro bayesiano si basa anche su un file di dati spam. Questo file deve includere un ampio campione di spam nota. Inoltre, deve essere costantemente aggiornato dal software antispam con lo spam più recente. In tal modo, si assicurerà che il filtro bayesiano sia consapevole delle ultime tendenze spam, portando così a un’elevata percentuale di rilevazione spam.

Realizzazione del filtro bayesiano

Una volta creati i database ham e spam, le probabilità della parola possono essere calcolate e il filtro è pronto all’uso.

Al momento in cui arriva il nuovo messaggio, viene suddiviso in parole e vengono rilevate quelle più pertinenti, dunque le più significative per l’identificazione del messaggio come spam o meno. Utilizzando queste parole, il filtro bayesiano calcola la probabilità che il nuovo messaggio sia spam. Se la probabilità è superiore a una determinata soglia, il messaggio viene classificato come spam.

> **NOTA**
> Per ulteriori informazioni sul filtro bayesiano e i relativi vantaggi, fare riferimento a:
> http://go.gfi.com/?pageid=ME_Bayesian

Addestramento del filtro analisi bayesiana

> **NOTA**
> Il filtro analisi bayesiana può essere addestrato anche utilizzando le cartelle pubbliche. Per ulteriori informazioni, fare riferimento a Configurazione del filtro bayesiano (pagina 139)..

Per un certo periodo di tempo, è consigliabile eseguire il training del filtro Analisi bayesiana con il flusso di posta dell'organizzazione. Tramite la Procedura guidata analisi bayesiana è anche possibile eseguire il training di Analisi bayesiana con le e-mail inviate o ricevute prima dell'installazione di GFI MailEssentials. Ciò consente l'abilitazione immediata di Analisi bayesiana.

La seguente procedura guidata analizza le origini di:

» posta attendibile: ad esempio la cartella posta inviata di una cassetta postale

» messaggi spam: ad esempio la cartella di una cassetta postale dedicata ai messaggi spam

Passaggio 1: installazione della Procedura guidata analisi bayesiana

La Procedura guidata analisi bayesiana può essere installata in:

» Un computer che comunica con Microsoft® Exchange, per analizzare la posta presente in una cassetta postale.

» Un computer dove è installato Microsoft Outlook, per l'analisi della posta di Microsoft Outlook.

Installazione della Procedura guidata analisi bayesiana:

1. Copiare il file di installazione **Bayesian Analysis Wizard.exe** nel computer selezionato. Questa cartella si trova in: GFI MailEssentials *percorso di installazione\AntiSpam\BSW*

2. Avviare **Bayesian Analysis Wizard.exe**.

3. Nella schermata iniziale, scegliere la lingua e rivedere il contratto di licenza con l'utente finale. Fare clic su **Avanti**.

4. Selezionare la cartella di installazione e fare clic su **Avanti**.

5. Per avviare l'installazione, fare clic su **Installa**.

6. Al completamento dell'installazione, fare clic su **Fine**.

Passaggio 2: analisi messaggi di posta attendibli e spam

Per avviare l'analisi dei messaggi mediante Procedura guidata analisi bayesiana:

1. Caricare Procedura guidata di analisi bayesiana da **Start > Tutti i programmi > GFI MailEssentials > GFI MailEssentials - Procedura guidata analisi bayesiana**.

2. Fare clic su **Avanti** nella schermata di benvenuto.

3. Scegliere se:

» Creare un nuovo file di profilo spam bayesiano (.bsp) oppure aggiornare uno esistente. Specificare il percorso di archiviazione del file e il nome file.

» Aggiornare direttamente il profilo spam bayesiano utilizzato dal filtro Analisi bayesiana al momento di eseguire l'installazione sullo stesso computer dove si trova GFI MailEssentials.

Fare clic su **Avanti** per continuare.

4. Scegliere in che modo la procedura guidata accederà alla posta attendibile. Selezionare:

» **Utilizzare il profilo Microsoft Outlook configurato su questo computer**: la posta viene recuperata da una cartella della posta di Microsoft Outlook. Per poter utilizzare questa opzione, Microsoft Outlook deve essere in esecuzione.

» **Connettersi all'archivio cassette postali di Microsoft ®Exchange Server**: i messaggi vengono recuperati da una cassetta postale di Microsoft® Exchange. Nella schermata successiva, specificare le credenziali di accesso.

» **Non aggiornare la posta attendibile (ham) nel profilo spam bayesiano**: viene saltato il recupero della posta attendibile. Andare al passaggio 6.

Per continuare, fare clic su **Avanti**.

5. Una volta che la procedura guidata si connette all'origine, scegliere la cartella contenente l'elenco della posta attendibile (ad es. la cartella Posta inviata), quindi fare clic su **Avanti**.

6. Selezionare in che modo la procedura guidata accederà all'origine dei messaggi spam. Selezionare:

» **Scaricare il profilo spam più recente dal sito Web GFI**: viene scaricato un file profilo spam che viene aggiornato regolarmente mediante la raccolta della posta dai siti di archivio spam di riferimento. È necessaria la connessione a Internet.

» **Utilizzare il profilo Microsoft Outlook configurato su questo computer**: lo spam viene recuperato da una cartella della posta di Microsoft Outlook. Per poter utilizzare questa opzione, Microsoft Outlook deve essere in esecuzione.

» **Connettersi all'archivio cassette postali di Microsoft ®Exchange Server**: i messaggi spam vengono recuperati da una cassetta postale di Microsoft® Exchange. Nella schermata successiva, specificare le credenziali di accesso.

» **Non eseguire l'aggiornamento spam nel profilo spam bayesiano**: viene saltato il recupero dei messaggi spam. Andare al passaggio 8.

Per continuare, fare clic su **Avanti**.

7. Dopo che la procedura guidata si collega all'origine, selezionare la cartella contenente l'elenco dei messaggi spam, quindi fare clic su **Avanti**.

8. Per avviare il recupero delle origini specificate, fare clic su **Avanti**. L'operazione potrebbe richiedere alcuni minuti.

9. Fare clic su **Fine** per chiudere la procedura guidata.

Passaggio 3: importazione del profilo spam bayesiano

Se la procedura guidata non viene eseguita sul server GFI MailEssentials, importare il file di profilo spam bayesiano (.bsp) in GFI MailEssentials.

1. Spostare il file nella cartella **Data** del percorso di installazione di GFI MailEssentials.

2. Riavviare i servizi **GFI MailEssentials AS Scan Engine** e **GFI MailEssentials Legacy Attendant**.

14 Glossario

A

Active Directory
Tecnologia che fornisce numerosi servizi di rete, inclusi servizi per directory LDAP.

AD
Vedere Active Directory

Archivi ricorsivi
Archivi che contengono livelli multipli di archivi secondari (archivi contenuti all'interno di altri). Noti anche come archivi nidificati.

B

BITS
Vedere Servizio trasferimento intelligente in background

Block list
Un elenco di indirizzi di posta elettronica da cui gli utenti non devono ricevere posta.

Blocklist in tempo reale
Database online di indirizzi IP spam. I messaggi in entrata vengono confrontati a questi elenchi per determinare se provengono da utenti bloccati.

Botnet
Una rete di computer infetti che sono eseguiti in modo autonomo e controllati da un hacker/cracker.

C

Cartella pubblica
Una cartella comune che consente agli utenti di Microsoft Exchange di condividere le informazioni.

CIDR
Vedere Classless Inter-Domain Routing

Classless Inter-Domain Routing
Una notazione di impostazione indirizzi IP che definisce un intervallo di indirizzi IP.

Comandi remoti
Istruzioni che facilitano la possibilità di eseguire in remoto le attività.

Crittografia PGP
Un sistema crittografico a chiave pubblica spesso utilizzato per crittografare i messaggi.

D

Demilitarized Zone

Un segmento di una rete con connessione a Internet che non fa parte della rete interna. Normalmente ha lo scopo di fungere da gateway tra le reti interne e Internet.

DMZ

Vedere Demilitarized Zone

DNS

Vedere Domain Name System

DNS MX

Vedere Mail Exchange

Domain Name System

Un database utilizzato dalle reti TCP/IP che consente la traduzione dei nomi host in indirizzi IP e di fornire altre informazioni relative al dominio.

E

Exploit

Un metodo di attacco che sfrutta le vulnerabilità note delle applicazioni e dei sistemi operativi allo scopo di compromettere la sicurezza del sistema.

F

Falsi negativi

Messaggi di spam che non vengono rilevati come tali.

Falsi positivi

Messaggi legittimi che vengono erroneamente identificati come spam.

Feed RSS

Un protocollo utilizzato per la distribuzione di contenuto (feed) ad aggiornamento frequente (ad esempio le news) con i relativi iscritti.

Filtro bayesiano

Una tecnica antispam in cui un indice statistico di probabilità addestrato dagli utenti viene utilizzato per l'identificazione dello spam.

Filtro greylist

Un filtro antispam che blocca i messaggi di posta spediti dagli spammer che non inviano nuovamente il messaggio quando ricevono un messaggio per un nuovo tentativo.

G

Gateway

Il computer (server) di una LAN che è direttamente connesso a una rete esterna. In GFI MailSecurity, gateway indica i server della posta all'interno dell'azienda che ricevono per primi la posta dai domini esterni.

H

Ham

Posta attendibile

HTTP

Protocollo di trasferimento HyperText: un protocollo utilizzato per il trasferimento dei dati ipertestuali tra server e browser internet.

I

IIS

Vedere Internet Information Services

IMAP

Vedere Internet Message Access Protocol.

Internet Information Services

Una serie di servizi basati su Internet creati da Microsoft Corporation per i server di Internet.

Internet Message Access Protocol

Uno dei due protocolli standard Internet più comuni per il recupero della posta elettronica. L'altro protocollo è POP3.

Intestazioni email

Informazioni che precedono il testo (corpo) del messaggio all'interno di un messaggio di posta. Le informazioni includono il mittente, il destinatario, l'oggetto, la data e l'ora di invio e ricezione e così via.

L

LDAP

Vedere Lightweight Directory Access Protocol

Liberatoria

Un'istruzione intesa a identificare o limitare la serie di diritti e obblighi dei destinatari della posta.

Lightweight Directory Access Protocol

Un protocollo di applicazione utilizzato per eseguire query e modificare i servizi di directory in esecuzione su TCP/IP.

M

Mail Exchange

Il record DNS utilizzato per identificare gli indirizzi IP dei server della posta del dominio.

Malware

Tutti i tipi dannosi di software che sono studiati per compromettere la sicurezza del computer e che solitamente si diffondono con metodi dannosi.

MAPI

Vedere Messaging Application Programming Interface

MDAC

Vedere Microsoft Data Access Components

Messaging Application Programming Interface

Architettura per la messaggistica e API COM (Component Object Model) per Microsoft Exchange.

Microsoft Data Access Components

Una tecnologia Microsoft che offre agli sviluppatori un modo uniforme e coerente di sviluppare software in grado di accedere a quasi qualsiasi archivio dati.

MIME

Vedere Multipurpose Internet Mail Extensions.

Motore di decompressione

Un modulo di scansione che decomprime e analizza gli archivi (ad esempio, file .zip e .rar) allegati a un messaggio.

Motore di scansione antivirus

Una tecnologia di rilevazione antivirus implementata all'interno del software antivirus che è responsabile della rilevazione effettiva dei virus.

MSMQ

Vedere Servizi Microsoft Message Queuing

Multipurpose Internet Mail Extensions

Standard che estende il formato della posta elettronica per supportare altri formati di testo oltre ad ASCII, allegati non di testo, corpi dei messaggi con più parti e informazioni delle intestazioni in gruppi di caratteri diversi da ASCII.

N

NDR

Vedere rapporto di mancato recapito

O

Operazioni spam

Azioni effettuate sui messaggi spam ricevuti, ad esempio l'eliminazione di posta o l'invio alla cartella di posta indesiderata.

P

Phishing

Il processo di acquisizione di informazioni personali sensibili allo scopo di defraudare le persone, solitamente attraverso l'uso di comunicazioni false.

POP2Exchange

Un sistema che raccoglie i messaggi di posta dalle cassette postali POP3 e li inoltra al server di posta.

POP3

Vedere Post Office Protocol 3.

Post Office Protocol ver.3

Un protocollo client/server per l'archiviazione di messaggi così che i clienti possano connettersi al server POP3 in qualsiasi momento e leggere la posta. Un client di posta stabilisce una connessione TCP/IP con il server e, attraverso lo scambio di una serie di comandi, permette agli utenti di leggere la posta.

Q

Quarantena

Un database di posta dove i messaggi rilevati come spam e/o malware sono archiviati in un ambiente controllato. I messaggi inseriti in quarantena non rappresentano una minaccia all'ambiente di rete.

Quarantine Store

Un repository centrale all'interno di GFI MailSecurity dove sono conservati tutti i messaggi bloccati finché non sono rivisti da un amministratore.

R

Raccolta di directory

Attacchi di posta dove gli indirizzi di posta elettronica noti vengono utilizzati come modello per crearne di altri.

Rapporto di mancato recapito

Un messaggio di posta elettronico inviato in automatico al mittente in presenza di un problema di recapito.

RBL

Vedere Blocklist in tempo reale

Regole monitoraggio posta elettronica

Regole che consentono la replica dei messaggi tra gli indirizzi di posta elettronica.

Risposta automatica

Una risposta automatica che viene inviata in automatico ai messaggi in entrata.

S

Secure Sockets Layer

Un protocollo che garantisce comunicazioni integrali e sicure tra le reti.

server di elenco

Un server che distribuisce i messaggi di posta inviati a elenchi di discussione e di newsletter, gestendone anche le richieste di iscrizione.

Server perimetrale/gateway

L'host di una LAN che è direttamente connesso a una rete esterna. In GFI MailEssentials, gateway indica i server della posta all'interno dell'azienda che ricevono per primi la posta dai domini esterni.

Servizi Microsoft Message Queuing

Un'implementazione della coda dei messaggi per i sistemi operativi Windows Server.

Servizio trasferimento intelligente in background

Un componente dei sistemi operativi Microsoft Windows che facilita il trasferimento di file tra sistemi che utilizza larghezze di banda di rete inattive.

Simple Mail Transport Protocol

Uno standard Internet utilizzato per la trasmissione di posta elettronica tra le reti IP.

SMTP

Vedere Simple Mail Transport Protocol

Software antivirus

Software che rileva malware come trojan horse in messaggi, file e applicazioni.

SSL

Vedere Secure Sockets Layer

Strumento di disinfezione HTML

Un modulo di filtraggio all'interno di GFI MailSecurity che scansiona e rimuove il codice di script html dai messaggi.

T

Trojan horse

Software dannoso che compromette un computer camuffandosi da software attendibile.

W

WebDAV

Un’estensione di HTTP che consente agli utenti di gestire i file in remoto e in modo interattivo. Utilizzato per la gestione dei messaggi nella cassetta postale e nella cartella pubblica di Microsoft Exchange.

Whitelist

Un elenco di indirizzi di posta e domini da cui viene ricevuta la posta.

Z

Zombie

Un computer infetto che fa parte di una botnet attraverso il malware.

15 Indice

A

Active Directory 17, 21, 25, 33, 42, 50, 109, 115, 164, 171, 222, 228, 245, 248, 266, 275, 277

Aggiorna 60, 114, 147, 179, 217, 224, 261

Aggiornamenti 25, 48-49, 54-55, 60-61, 74, 77, 81, 85, 89, 93, 100, 103, 110, 115, 140, 242, 246-247, 272, 287-288

Analisi bayesiana 17, 25, 110, 138, 162-163, 242, 288, 293

Antispam 11, 15, 17, 20-21, 25, 32, 36, 47, 49, 56, 60, 64, 66, 109-110, 113, 115, 118, 120-121, 123, 125, 127, 129-130, 133, 137-138, 141, 144, 146, 148, 151-152, 154, 156-159, 162, 170, 174, 208, 213, 242, 246, 258, 266-267, 273, 277, 287, 292

Antivirus 16, 22, 24-25, 41, 49-50, 60, 74, 78, 82, 86, 90, 94, 200, 209, 214, 242, 281

B

Block list DNS IP 17, 25, 109, 123, 242

Block list DNS URI 17, 25, 109, 125, 242

Block list e-mail 17, 109, 118, 121, 159, 175, 242, 288

Block list IP 17, 109, 121, 242

C

Cluster 24, 26, 30, 73

Comandi remoti 16, 159, 287

Controllo intestazione 17, 110, 132-133, 242

Controllo parola chiave 137, 160, 242

D

Dashboard 11, 54-55, 58, 60-62, 286

Database 17, 35-36, 54, 56, 61-62, 67, 69, 72, 97, 109, 113, 118, 121, 130, 140, 159, 170, 234-235, 245, 273, 287, 289, 292

DEP 50

Directory virtuale 13, 43, 171, 225, 251-252, 267

DMZ 20, 26, 42, 171, 224

Dominio 11, 16, 26, 33, 42, 46, 50, 109, 115, 120, 124, 126-127, 129, 131, 135, 141, 160, 163, 166-168, 171, 224, 228, 231, 238, 244-245, 248, 266, 268, 286, 289

F

Feed RSS 216

Filtro allegati 17, 179, 183, 242, 245

Filtro messaggi in entrata 15

Filtro messaggi in uscita 15

firewall 20, 25, 41, 117, 171, 224, 288

G

gateway 19, 23-24, 26, 33, 41, 74, 78, 82, 86, 90, 126, 153, 207, 214, 256, 286, 290

Gestione licenze 246, 288

Greylist 18, 50, 110, 130, 153, 242, 289

I

IIS 21, 23, 26, 30, 34, 41, 130, 244, 246, 248, 251, 267, 274, 276, 286, 288

IMAP 37, 171, 287

Internet 15, 23, 27, 33, 45, 225, 240, 243, 263, 268, 288, 294

IP 17, 27, 33, 44, 71, 106, 109, 121, 123, 126, 129-130, 135, 144, 150, 224, 240, 243, 259, 289, 292

ISP 29, 33, 263

K

Kaspersky 16, 51, 74, 82

L

Liberatorie 12, 227, 230-231, 289

Lotus Domino 19, 25-26, 29, 32, 39, 170

Lotus Notes 29, 36

M

MAPI 170, 265

Microsoft Exchange 26, 150, 256, 263

Monitoraggio posta elettronica 12, 237

MSMQ 24

N

Net framework 165

Newsletter 32, 164, 174, 233-235

Nuovi mittenti 15, 18, 110, 145, 151, 242

O

Operazioni spam 148, 263, 275, 277

P

Phishing 265

POP2Exchange 31, 54-55, 62, 259, 274, 276

POP3 29, 259, 287

Posta attendibile 18, 50, 110, 117, 139, 141, 292

Prestazioni 28, 51, 71, 143, 247, 258, 281

Procedura guidata 41, 44, 48-49, 126, 141, 275, 277, 293

Q

Quarantena 11, 13, 16, 21, 43, 47, 52, 56, 59, 61, 76, 80, 84, 88, 92, 97, 102, 149, 180, 186, 193, 197, 203, 209, 213, 216, 218, 225, 249, 251, 254, 256, 284, 287

R

Raccolta di directory 15, 17, 50, 109, 115, 153, 242, 275, 277

risposte automatiche 12, 15, 231

S

Sender Policy Framework 17, 109-110, 126, 242, 289

Server DNS 44, 159

server perimetrale 20, 26, 107, 127

Server SMTP 27, 46, 127, 130, 239

Server virtuale SMTP 27

SpamRazer 17, 25, 109-110, 148, 242

T

Trasporto hub 13, 94

W

WebDAV 170

Whitelist 11, 16, 18, 21, 50, 105, 110-111, 120-121, 126, 129, 132, 135, 141, 144-145, 151, 159, 162, 170, 174, 242, 252, 288

STATI UNITI D'AMERICA, CANADA E AMERICA CENTRALE E DEL SUD

4309 Emperor Blvd, Suite 400, Durham, NC 27703, USA

Telefono: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

REGNO UNITO E REPUBBLICA D'IRLANDA

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, Regno Unito

Telefono: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPA, MEDIO ORIENTE E AFRICA

GFI House, Territorials Street, Mriehel BKR 3000, Malta

Telefono: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA E NUOVA ZELANDA

83 King William Road, Unley 5061, South Australia

Telefono: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

GFI®